FIG. 1

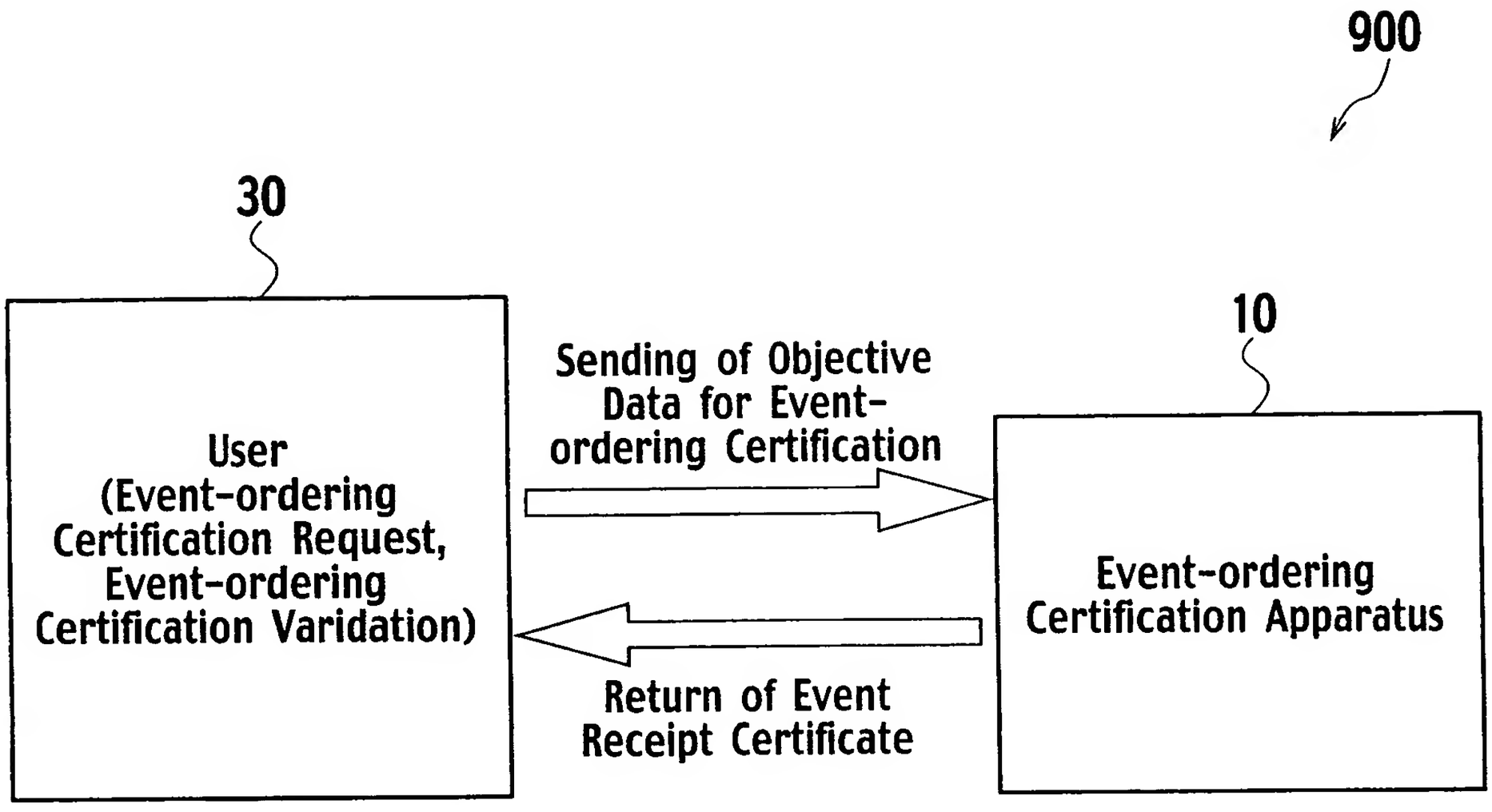

900
30
User
(Event-ordering
Certification Request,
Event-ordering
Certification Varidation)
Sending of Objective
Data for Event-
ordering Certification
Return of Event
Receipt Certificate
10
Event-ordering
Certification Apparatus

FIG. 2

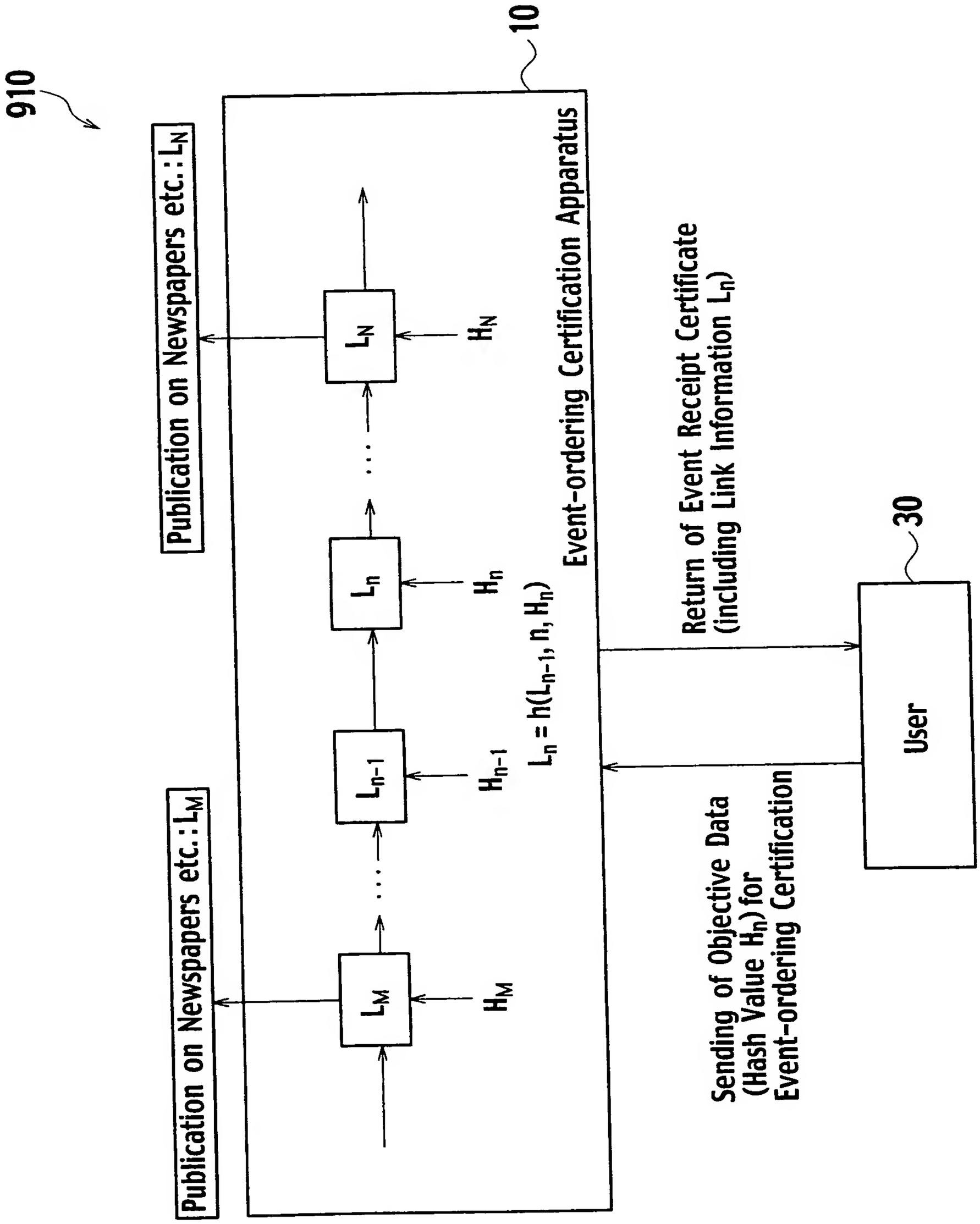

910
10
Publication on Newspapers etc.: L_N
L_N
H_N
L_n
H_n
L_{n-1}
H_{n-1}
$L_n = h(L_{n-1}, n, H_n)$
Publication on Newspapers etc.: L_M
L_M
H_M
Event-ordering Certification Apparatus
Return of Event Receipt Certificate
(including Link Information L_n)
30
User
Sending of Objective Data
(Hash Value H_n) for
Event-ordering Certification

FIG. 3

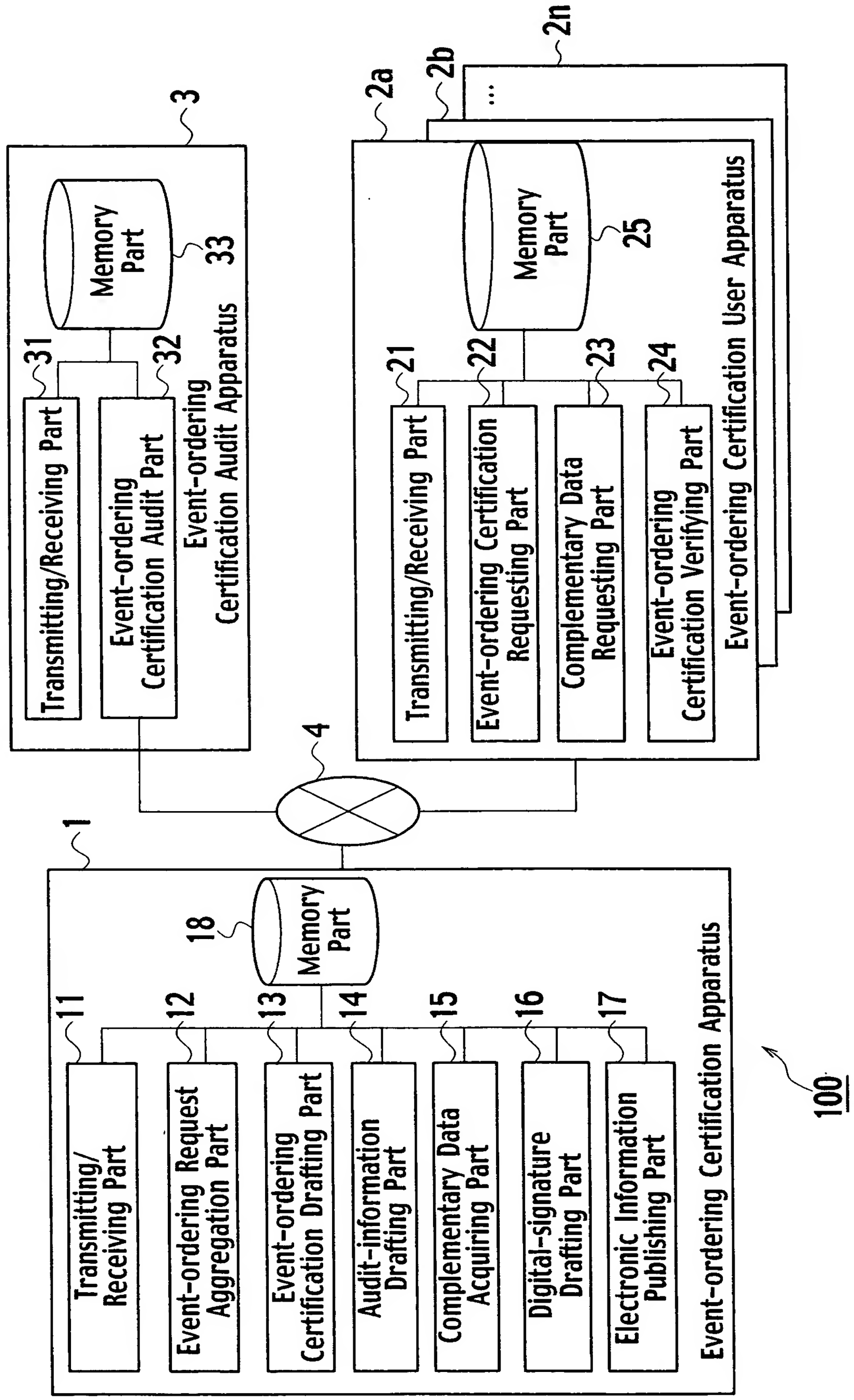
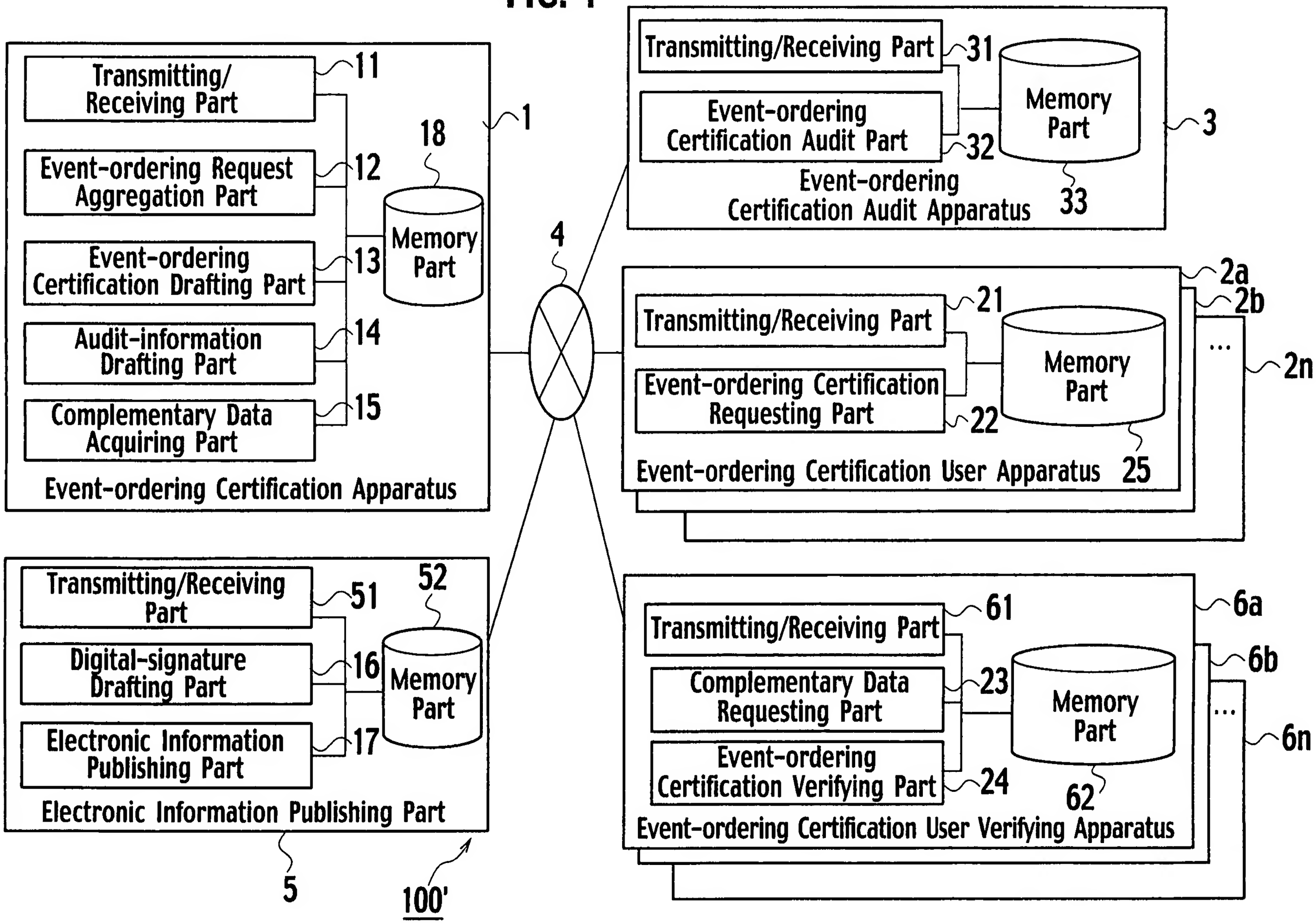
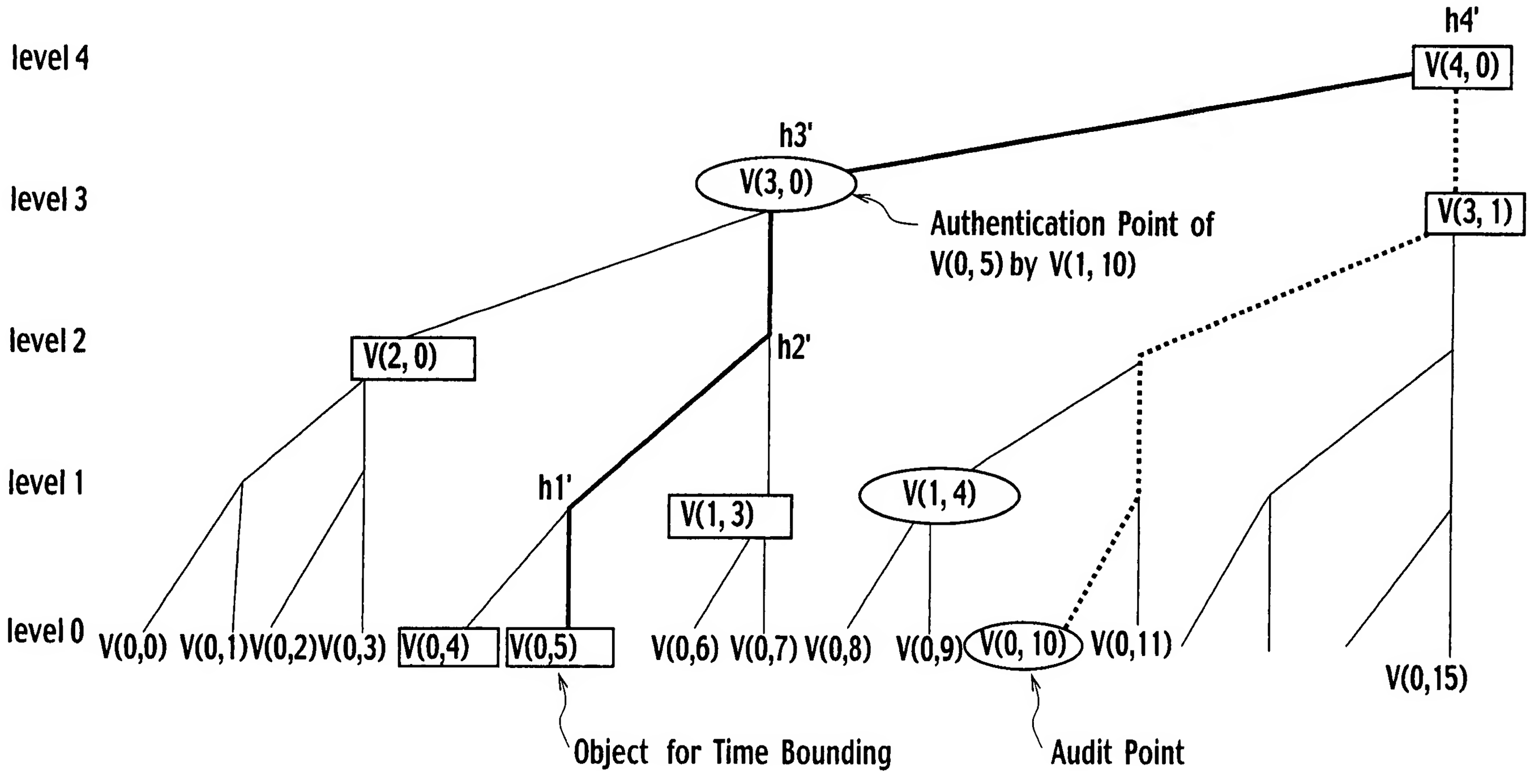

100
Event-ordering Certification Apparatus
11 Transmitting/ Receiving Part
12 Event-ordering Request Aggregation Part
13 Event-ordering Certification Drafting Part
14 Audit-information Drafting Part
15 Complementary Data Acquiring Part
16 Digital-signature Drafting Part
17 Electronic Information Publishing Part
18 Memory Part
1
4
Event-ordering Certification User Apparatus
21 Transmitting/Receiving Part
22 Event-ordering Certification Requesting Part
23 Complementary Data Requesting Part
24 Event-ordering Certification Verifying Part
25 Memory Part
2a
2b
2n
Event-ordering Certification Audit Apparatus
31 Transmitting/Receiving Part
32 Event-ordering Certification Audit Part
33 Memory Part
3

FIG. 4



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 4 of 77

FIG. 5



Inventors: Ellen McKiel
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4471/33867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 5 of 77

FIG. 6

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data (Positional Info. Assigned Value)	HK	
Digital Signature	DS	

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 7 of 77

FIG. 7

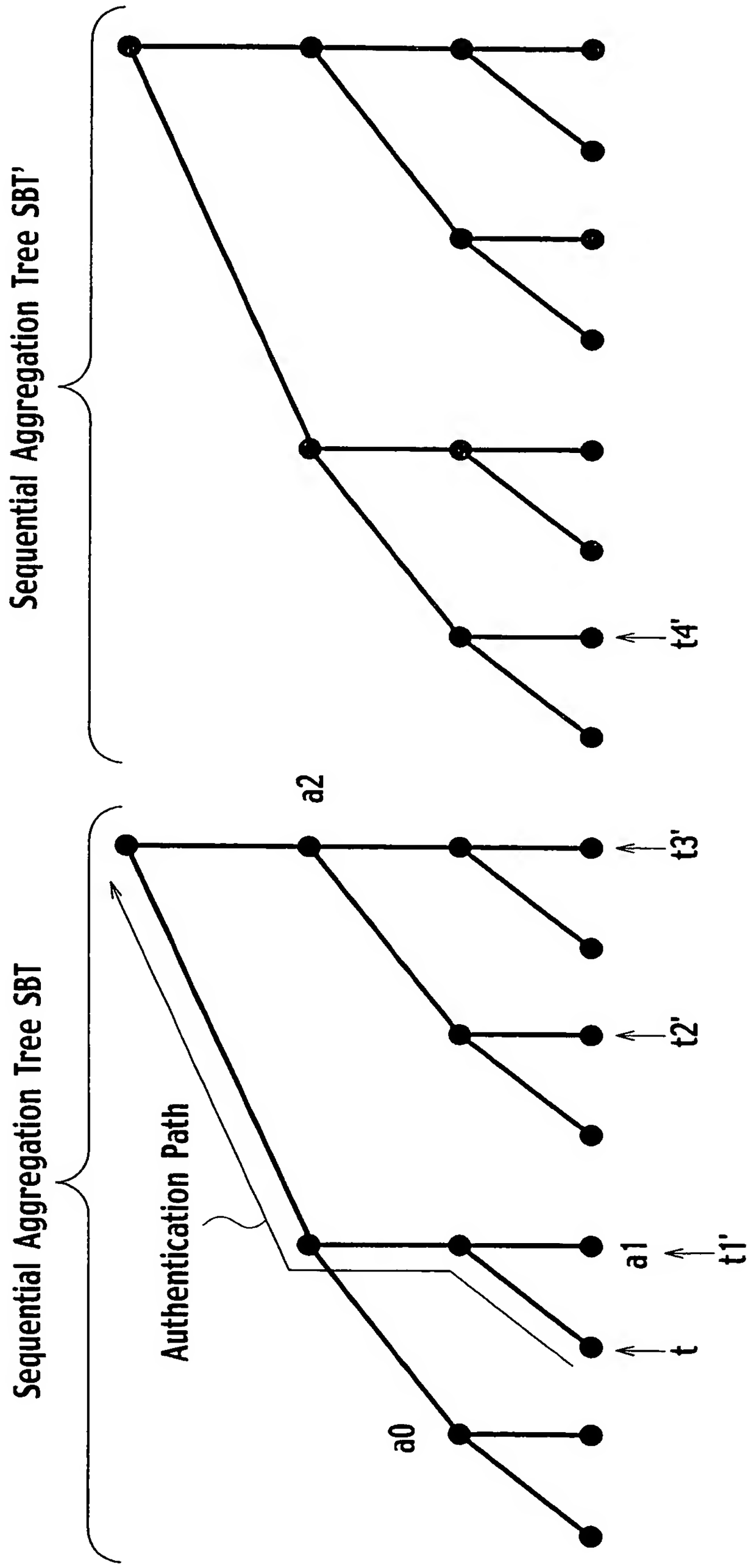
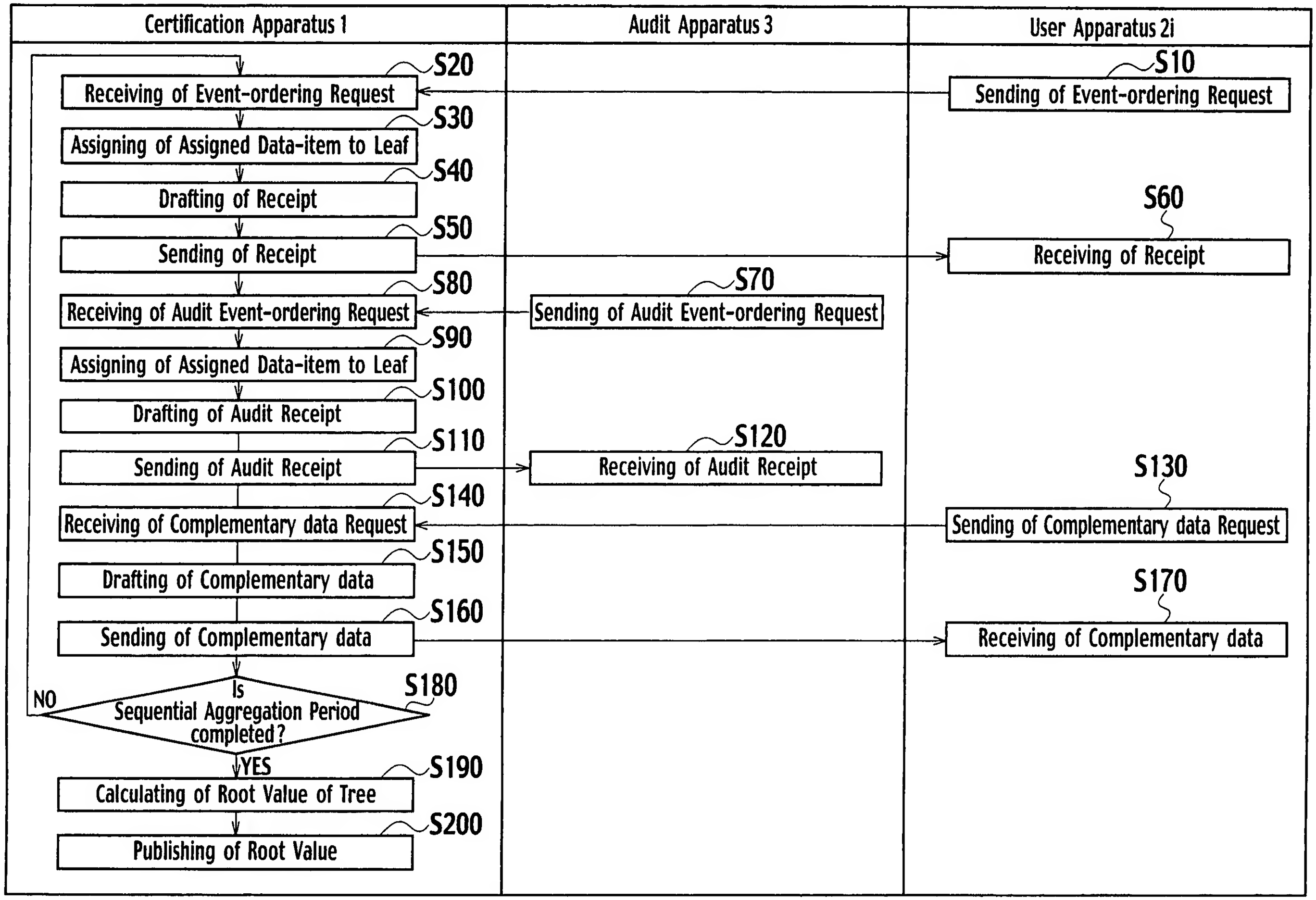


FIG. 8



Inventor: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4447/33286
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 8 of 77

FIG. 9

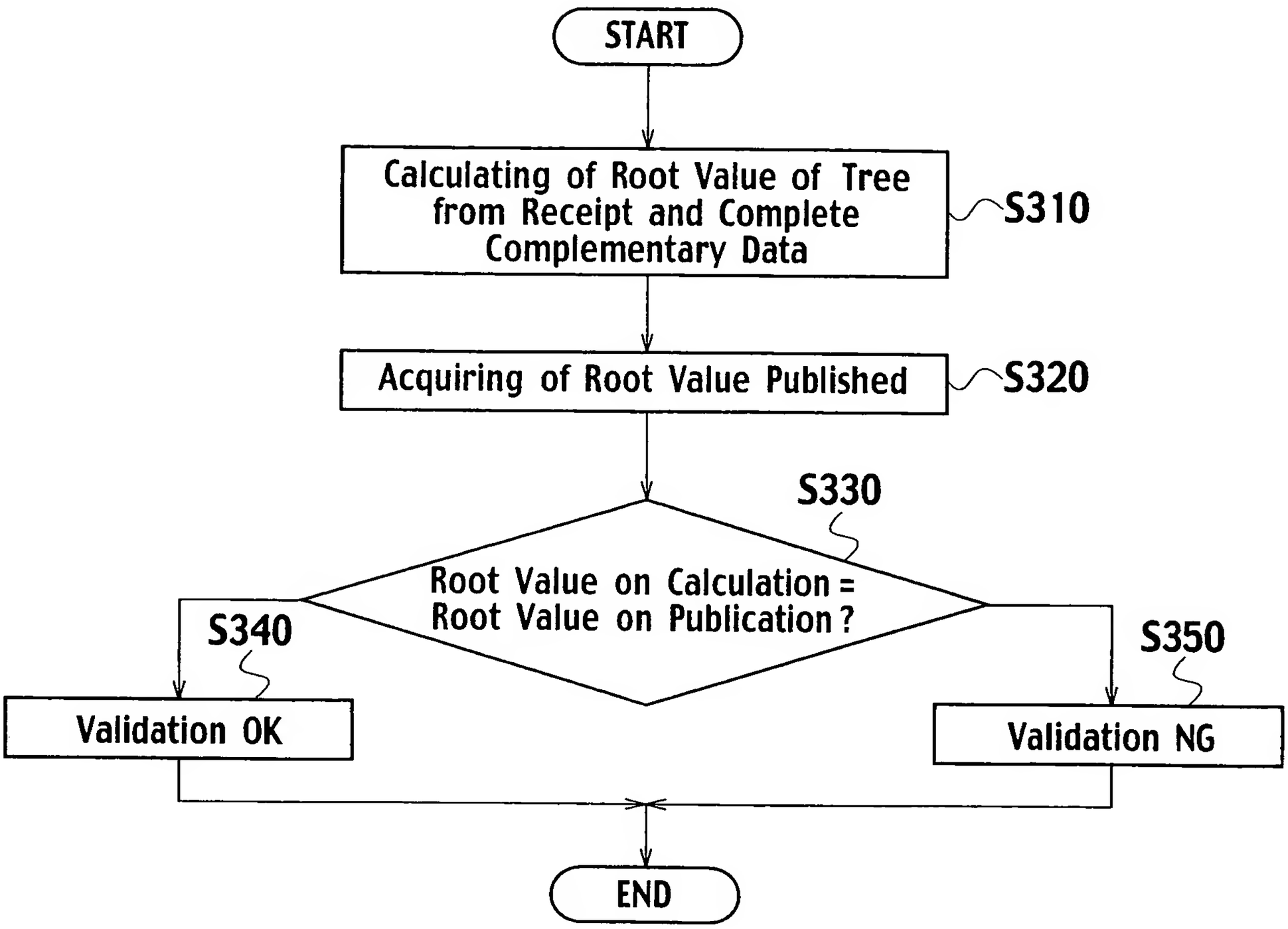
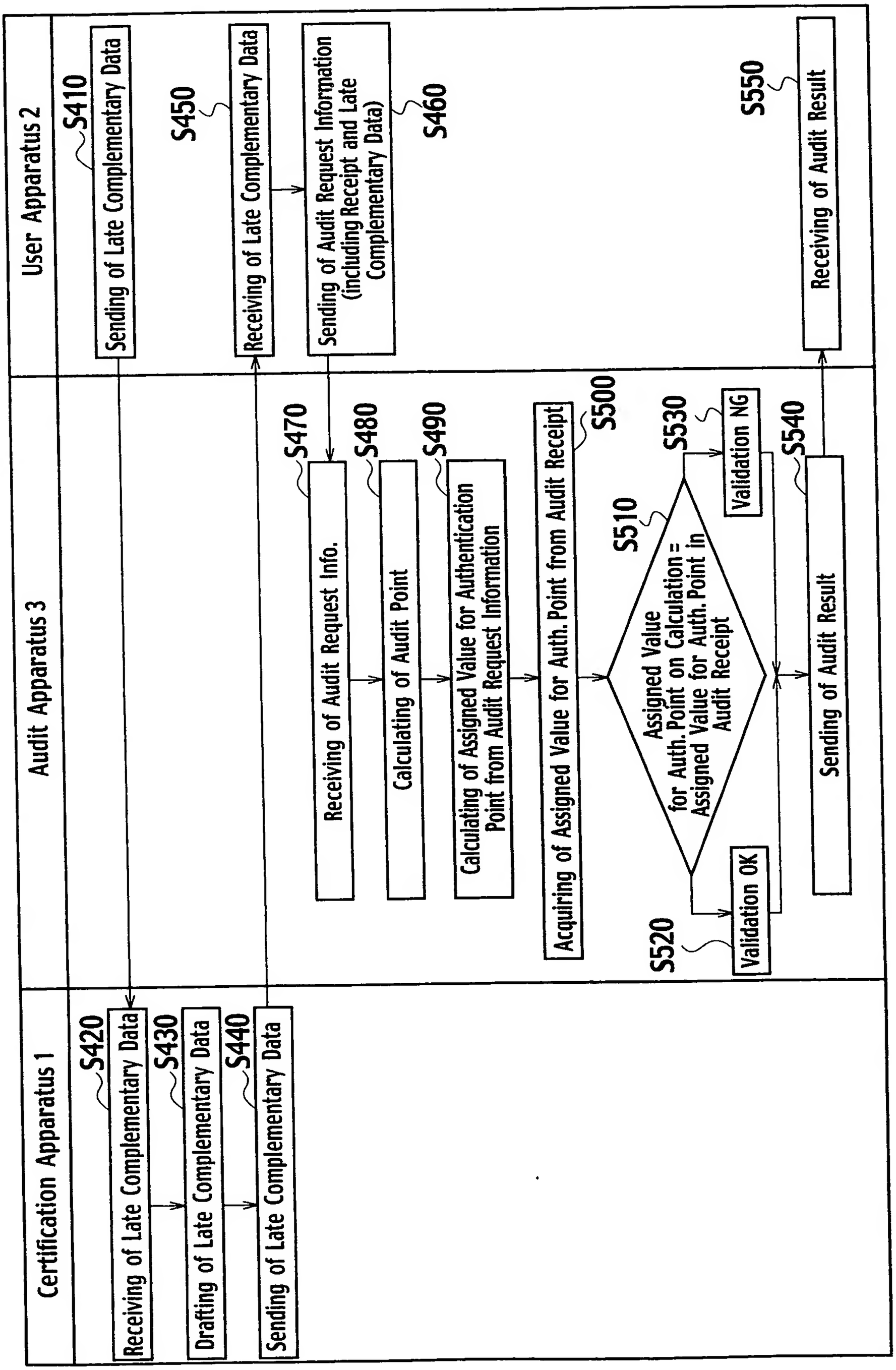

START
Calculating of Root Value of Tree from Receipt and Complete Complementary Data
S310
Acquiring of Root Value Published
S320
S330
Root Value on Calculation = Root Value on Publication ?
S340
Validation OK
S350
Validation NG
END

FIG. 10


User Apparatus 2
Audit Apparatus 3
Certification Apparatus 1
S410
Sending of Late Complementary Data
S450
Receiving of Late Complementary Data
S460
Sending of Audit Request Information (including Receipt and Late Complementary Data)
S550
Receiving of Audit Result
S470
Receiving of Audit Request Info.
S480
Calculating of Audit Point
S490
Calculating of Assigned Value for Authentication Point from Audit Request Information
S500
Acquiring of Assigned Value for Auth. Point from Audit Receipt
S510
Assigned Value for Auth. Point on Calculation = Assigned Value for Auth. Point in Audit Receipt
S520
Validation OK
S530
Validation NG
S540
Sending of Audit Result
S420
Receiving of Late Complementary Data
S430
Drafting of Late Complementary Data
S440
Sending of Late Complementary Data

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 11 of 77

FIG. 11

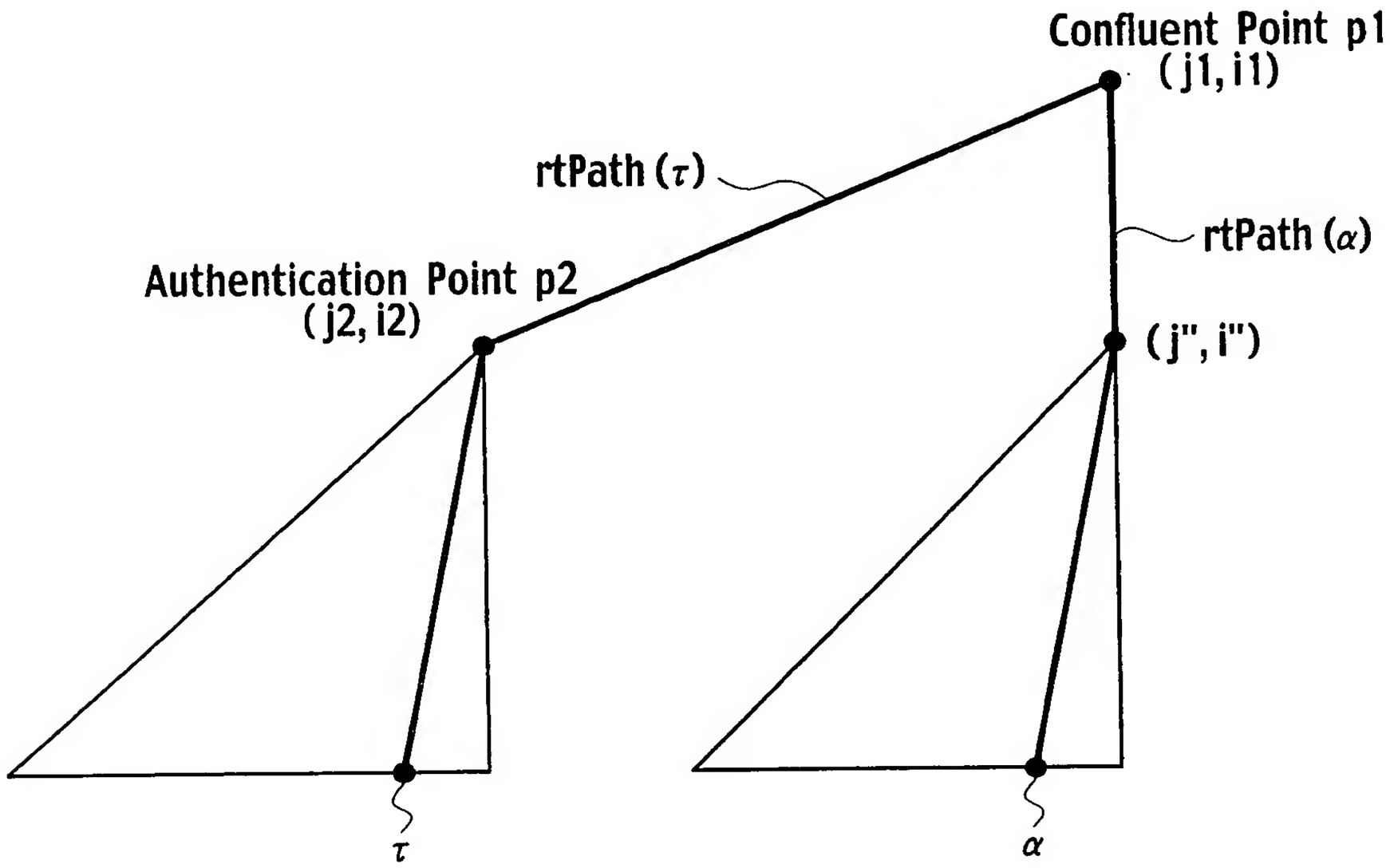


FIG. 12

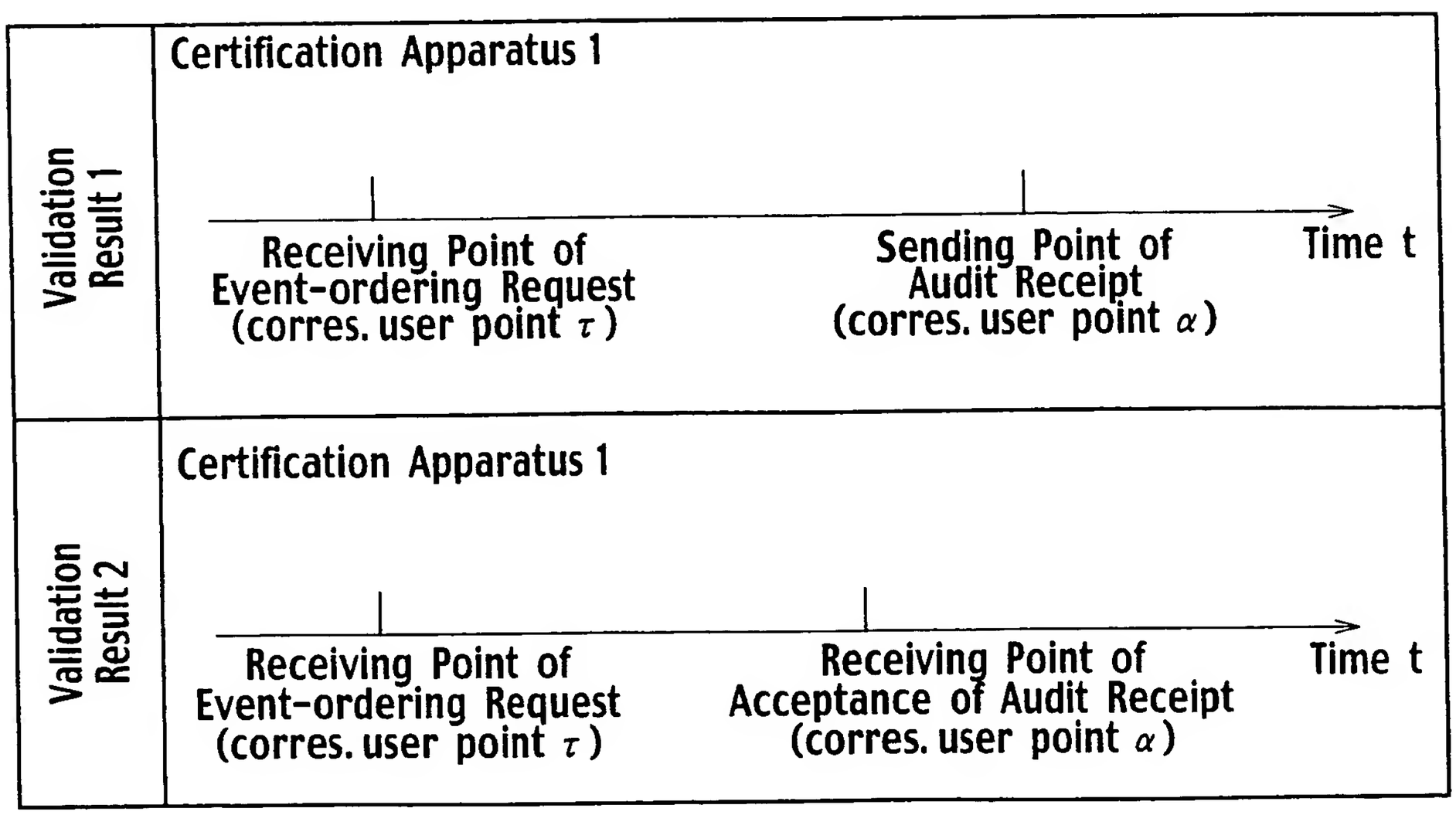
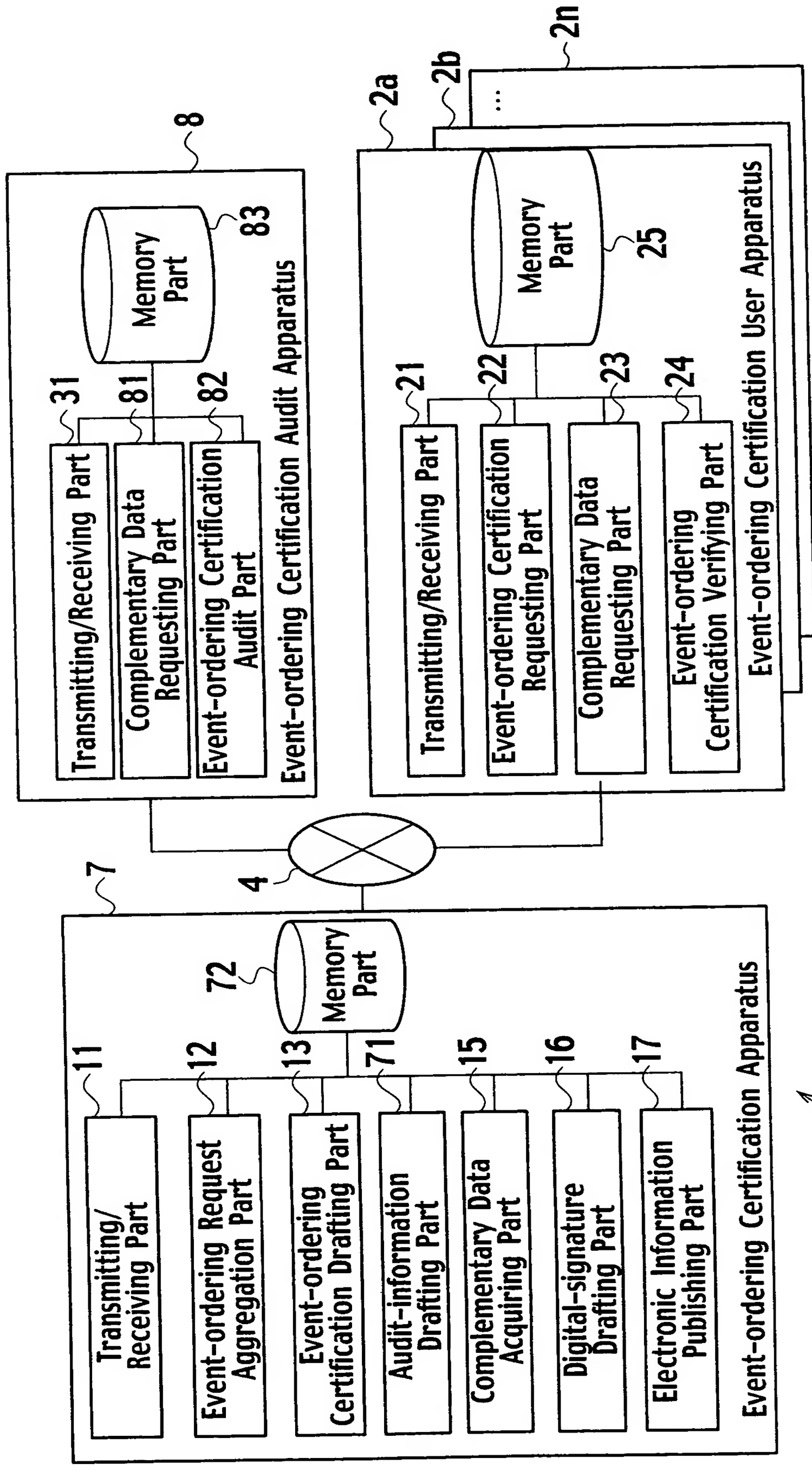
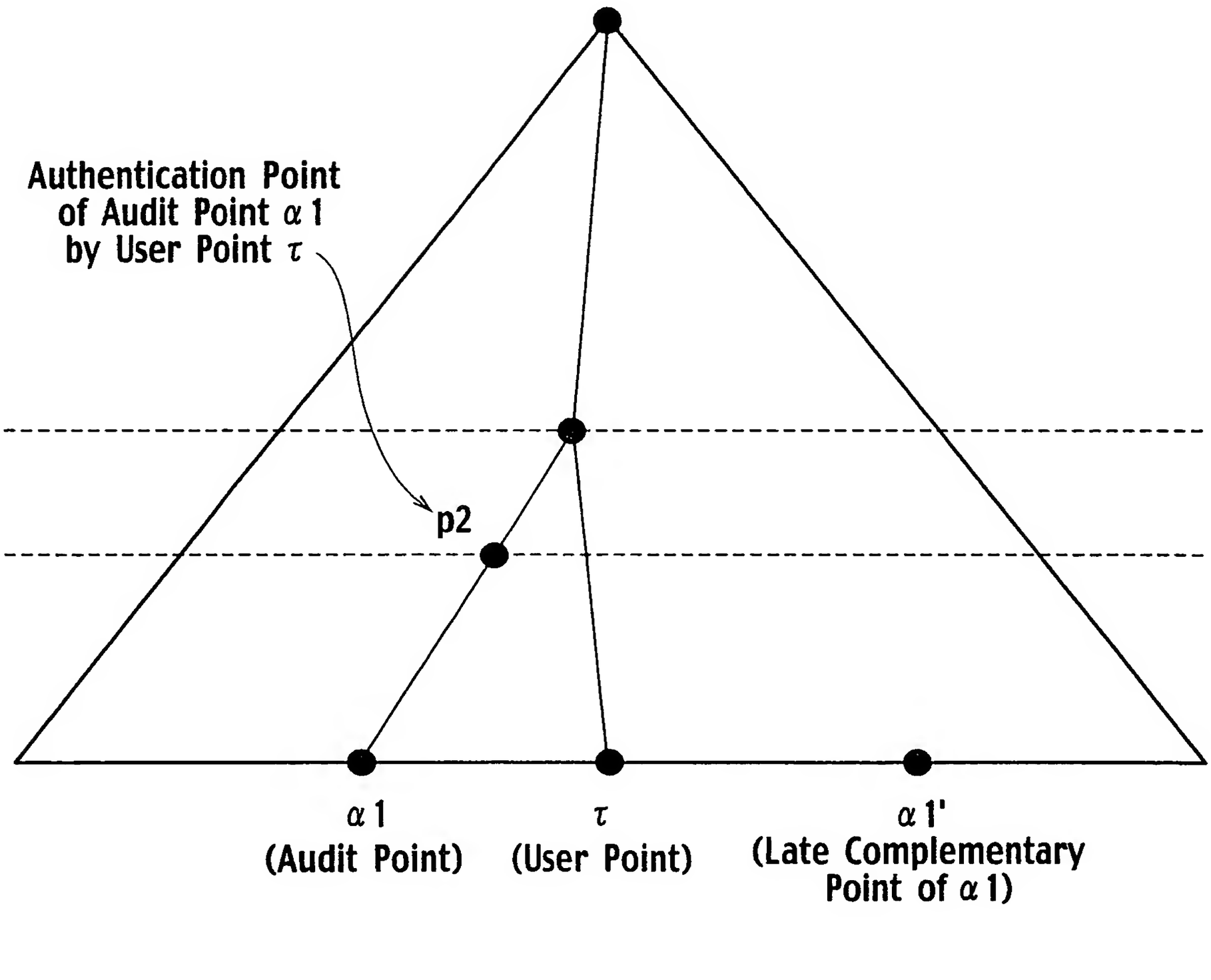


FIG. 13


8
83
Memory Part
31
81
82
Transmitting/Receiving Part
Complementary Data Requesting Part
Event-ordering Certification Audit Part
Event-ordering Certification Audit Apparatus
2a
2b
2n
25
21
22
23
24
Transmitting/Receiving Part
Event-ordering Certification Requesting Part
Complementary Data Requesting Part
Event-ordering Certification Verifying Part
User Apparatus
4
7
72
11
12
13
71
15
16
17
Transmitting/ Receiving Part
Event-ordering Request Aggregation Part
Event-ordering Certification Drafting Part
Audit-information Drafting Part
Complementary Data Acquiring Part
Digital-signature Drafting Part
Electronic Information Publishing Part
Event-ordering Certification Apparatus
200

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 13 of 77

FIG. 14



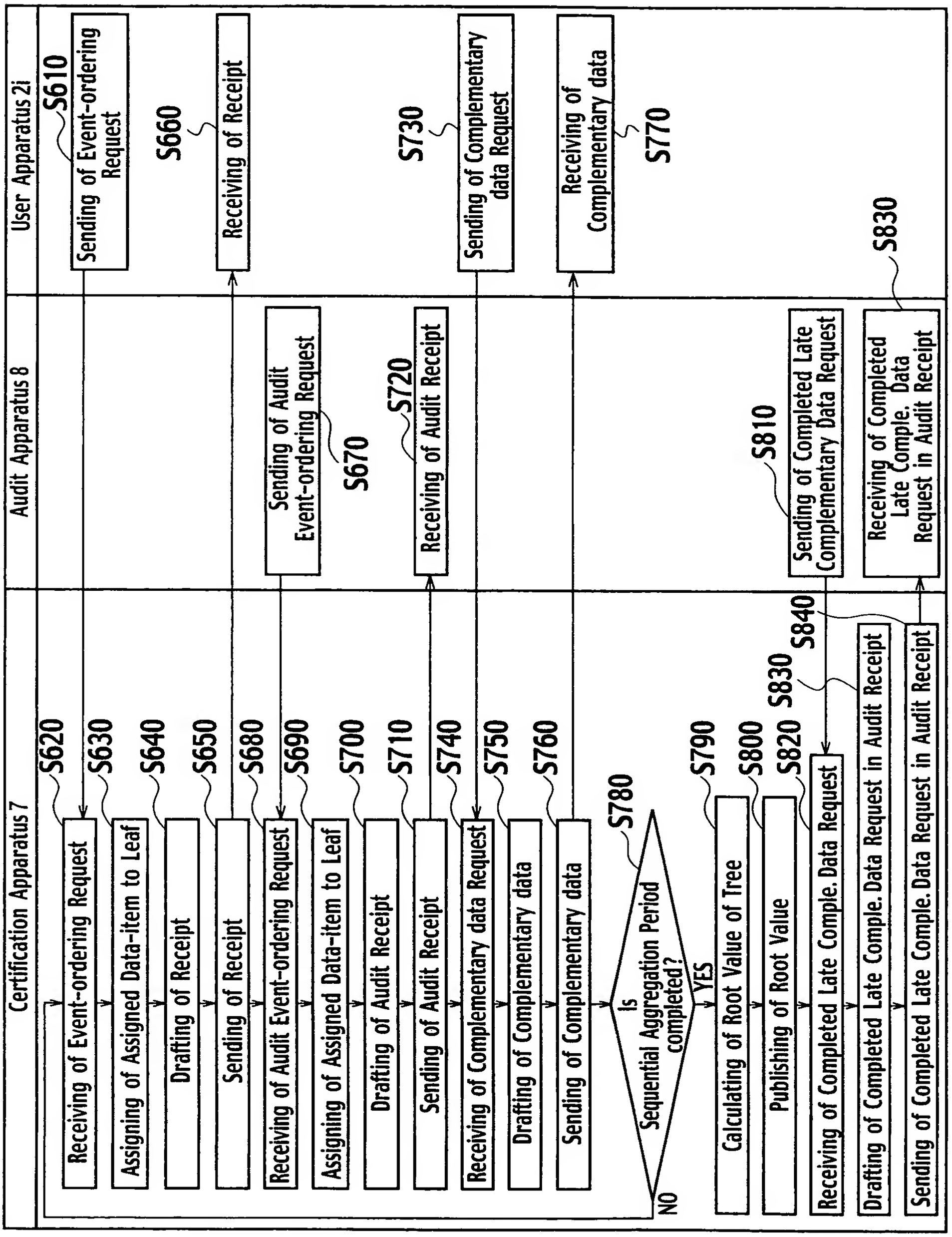
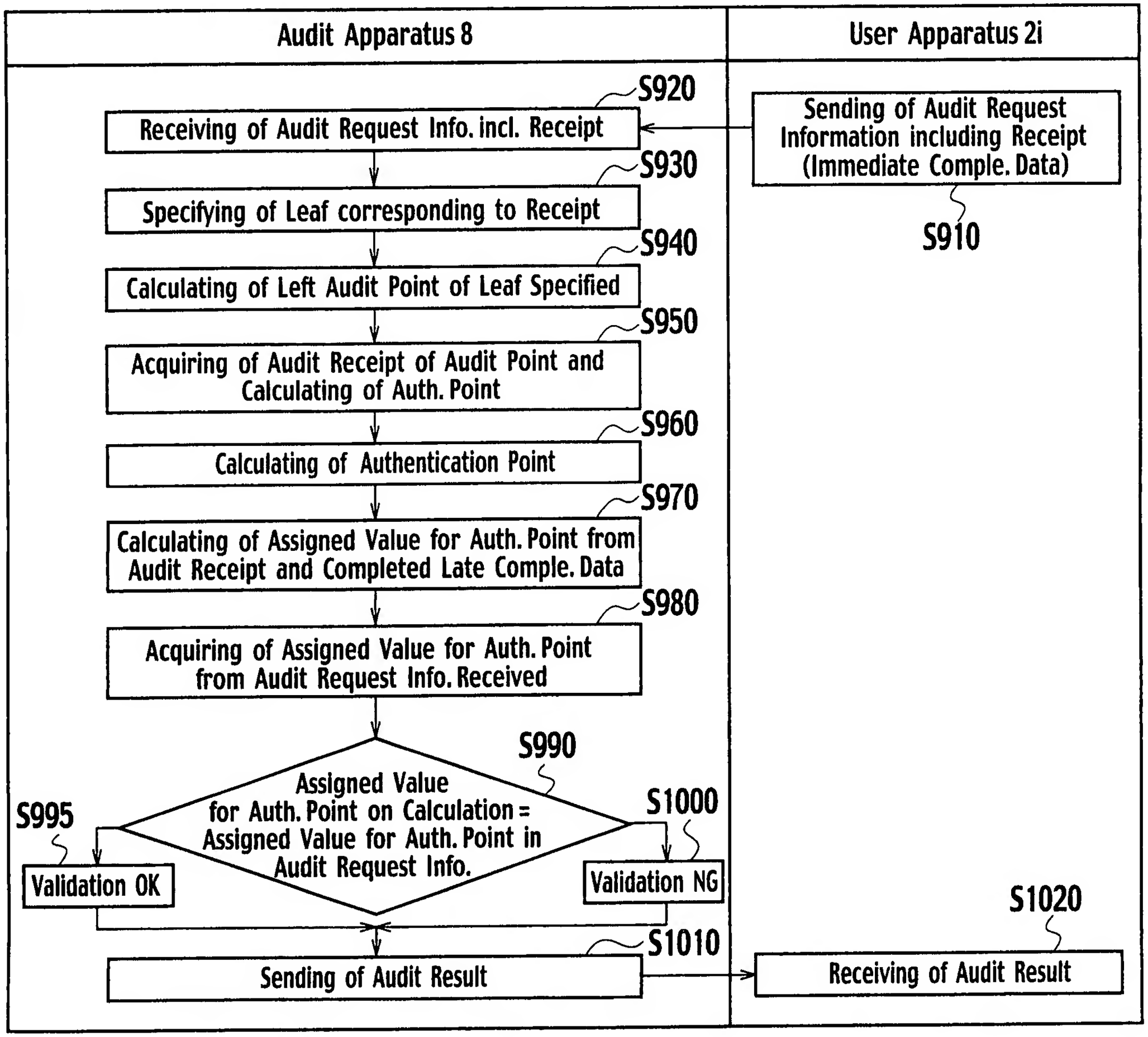

User Apparatus 2i
Audit Apparatus 8
Certification Apparatus 7
S610
Sending of Event-ordering Request
S660
Receiving of Receipt
S730
Sending of Complementary data Request
Receiving of Complementary data
S770
S830
S670
Sending of Audit Event-ordering Request
S720
Receiving of Audit Receipt
S810
Sending of Completed Late Complementary Data Request
Receiving of Completed Late Comple. Data Request in Audit Receipt
S620
Receiving of Event-ordering Request
S630
Assigning of Assigned Data-item to Leaf
S640
Drafting of Receipt
S650
Sending of Receipt
S680
Receiving of Audit Event-ordering Request
S690
Assigning of Assigned Data-item to Leaf
S700
Drafting of Audit Receipt
S710
Sending of Audit Receipt
S740
Receiving of Complementary data Request
S750
Drafting of Complementary data
S760
Sending of Complementary data
S780
Is Sequential Aggregation Period completed?
NO
YES
S790
Calculating of Root Value of Tree
S800
Publishing of Root Value
S820
Receiving of Completed Late Comple. Data Request
S830
Drafting of Completed Late Comple. Data Request in Audit Receipt
S840
Sending of Completed Late Comple. Data Request in Audit Receipt

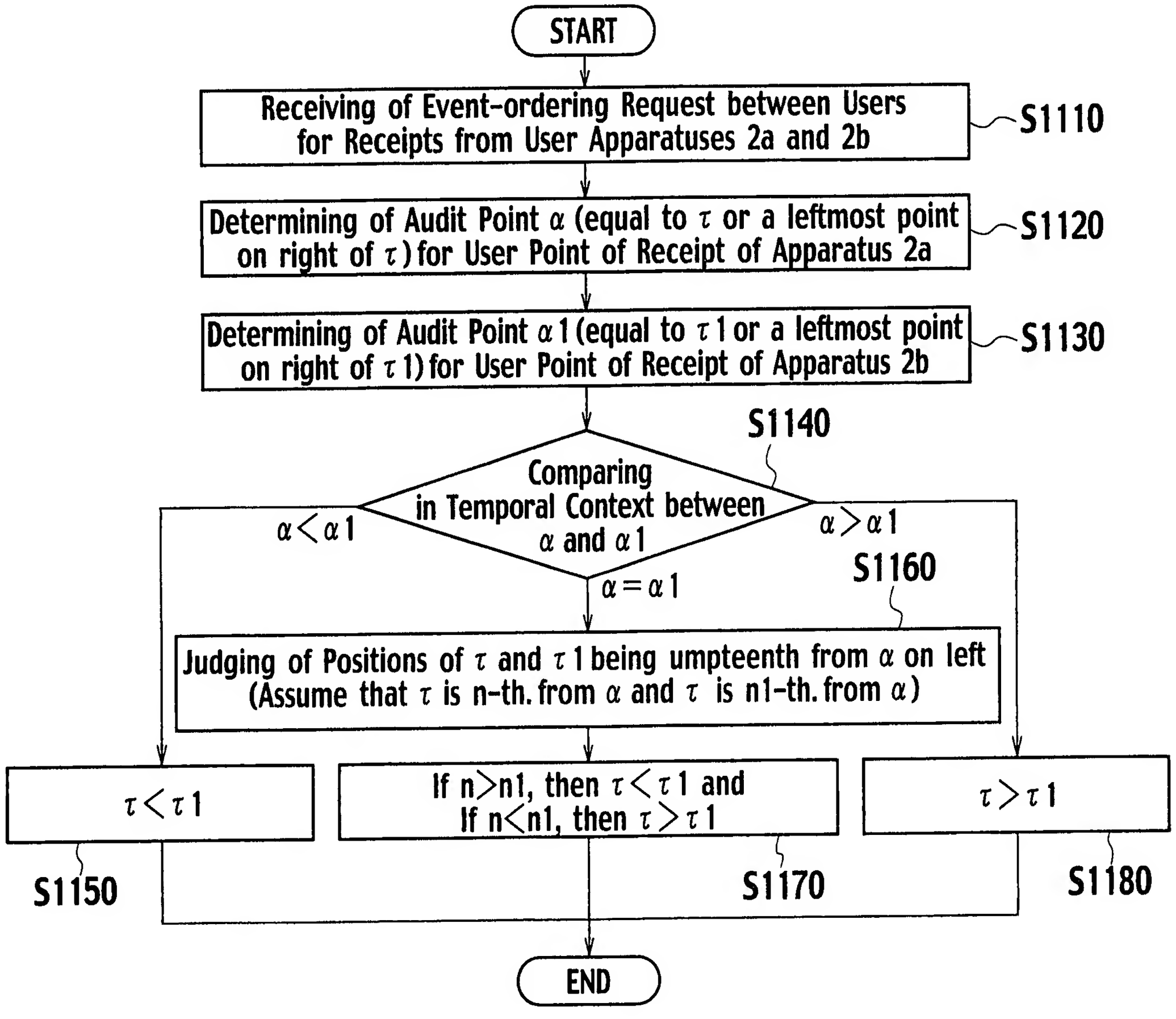
FIG. 15

FIG. 16



Inventors: Eiichi HOKUA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 15 of 77

FIG. 17



Inventor: Eiichi HONDA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4447/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 16 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 17 of 77

FIG. 18

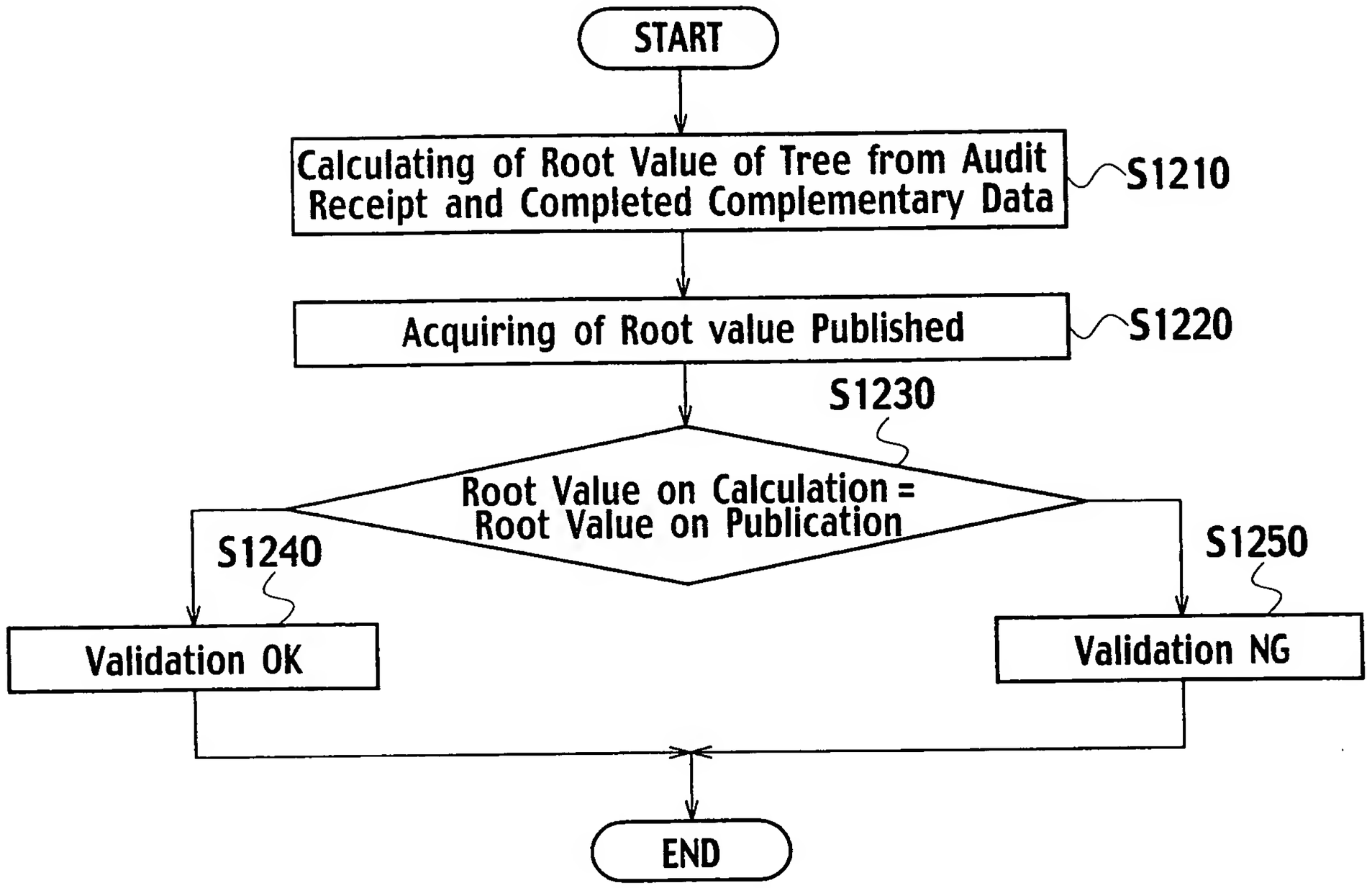


FIG. 19

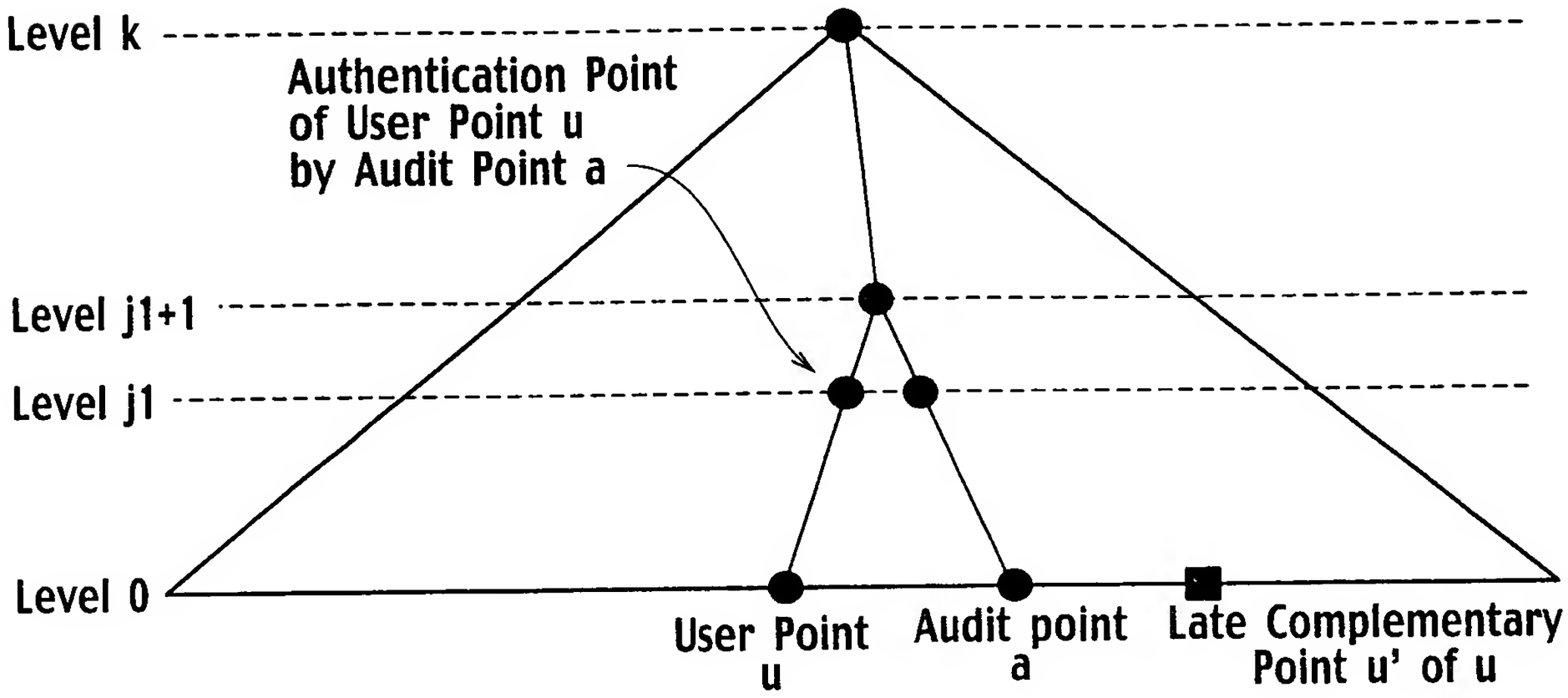

Level k
Authentication Point
of User Point u
by Audit Point a
Level j1+1
Level j1
Level 0
User Point
u
Audit point
a
Late Complementary
Point u' of u

FIG. 20

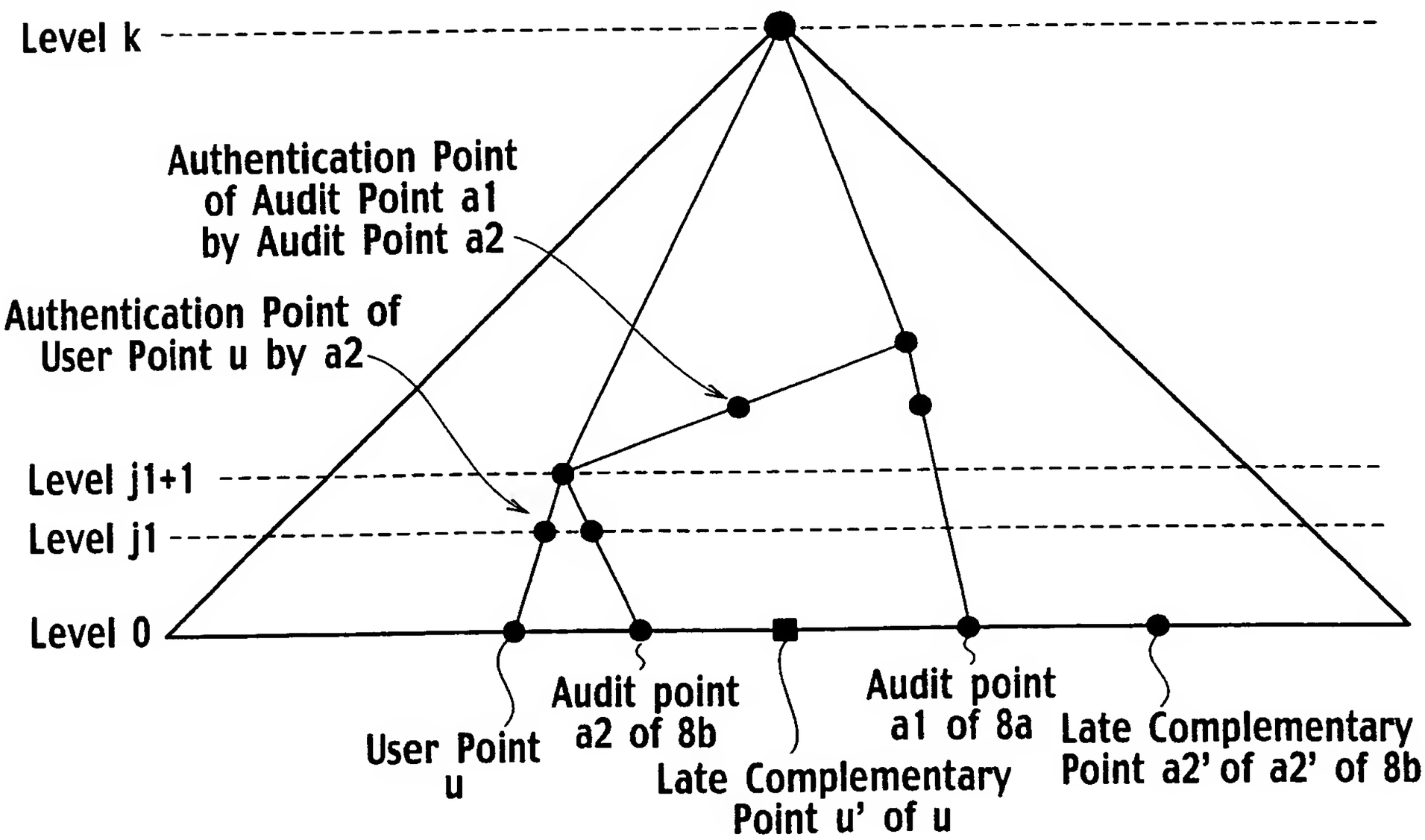
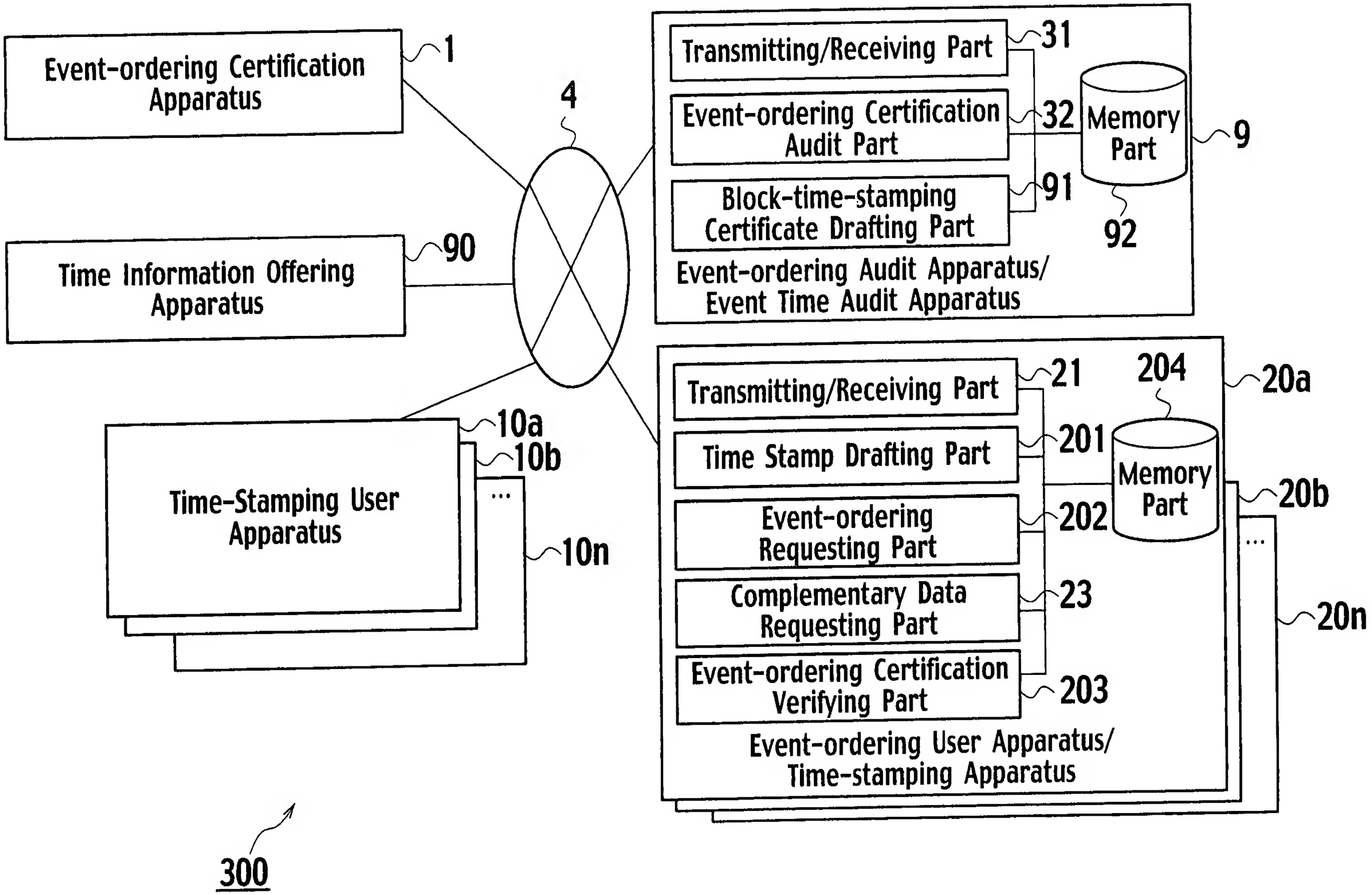

Level k
Authentication Point
of Audit Point a1
by Audit Point a2
Authentication Point of
User Point u by a2
Level j1+1
Level j1
Level 0
User Point
u
Audit point
a2 of 8b
Late Complementary
Point u' of u
Audit point
a1 of 8a
Late Complementary
Point a2' of a2' of 8b

FIG. 21



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4447/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 19 of 77

FIG. 22

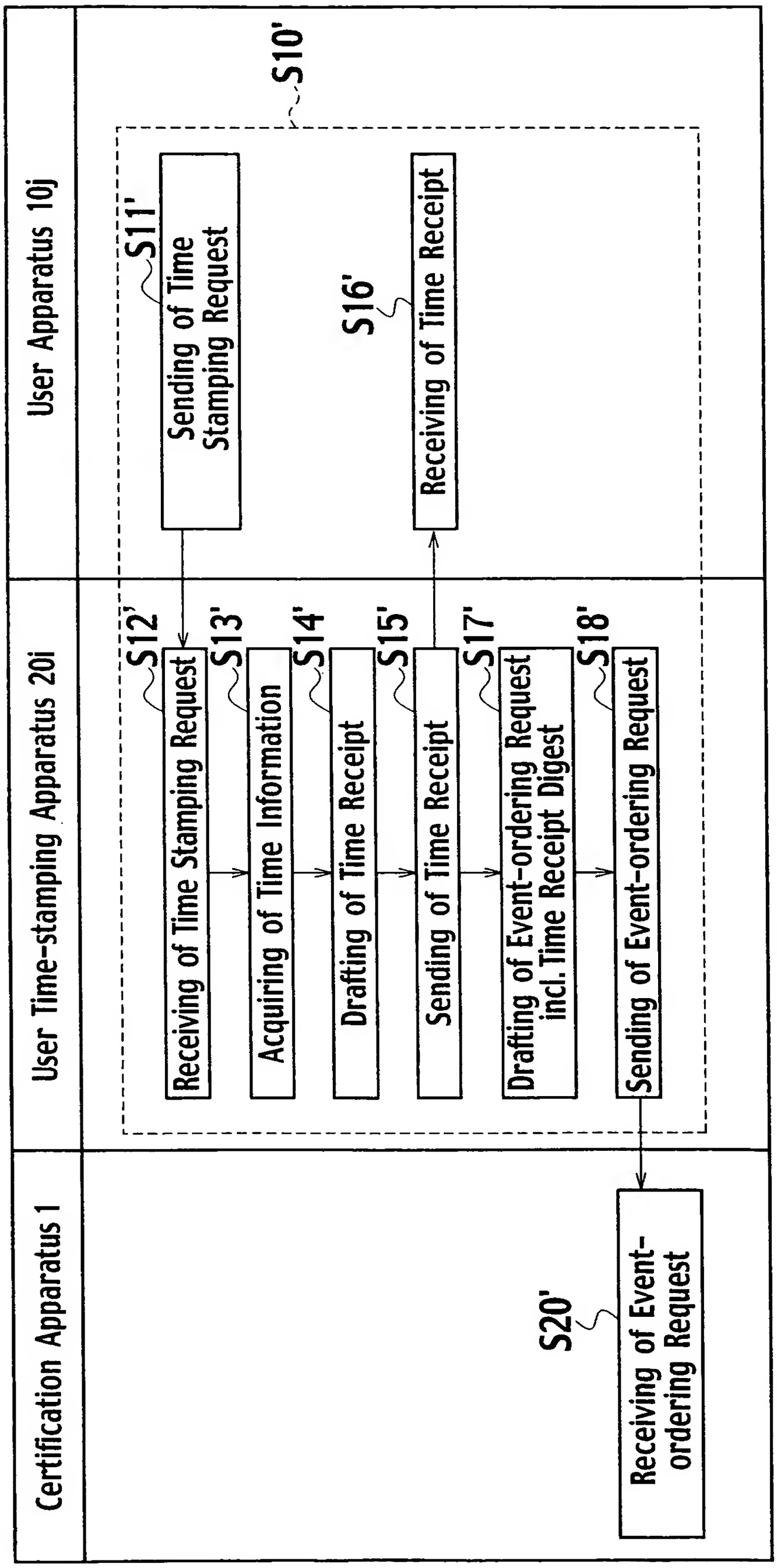

User Time-stamping Apparatus 10j
Certification Apparatus 1
User Time-stamping Apparatus 20i
S10'
S11'
Sending of Time Stamping Request
S12'
Receiving of Time Stamping Request
S13'
Acquiring of Time Information
S14'
Drafting of Time Receipt
S15'
Sending of Time Receipt
S16'
Receiving of Time Receipt
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S18'
Sending of Event-ordering Request
S20'
Receiving of Event-ordering Request

FIG. 23

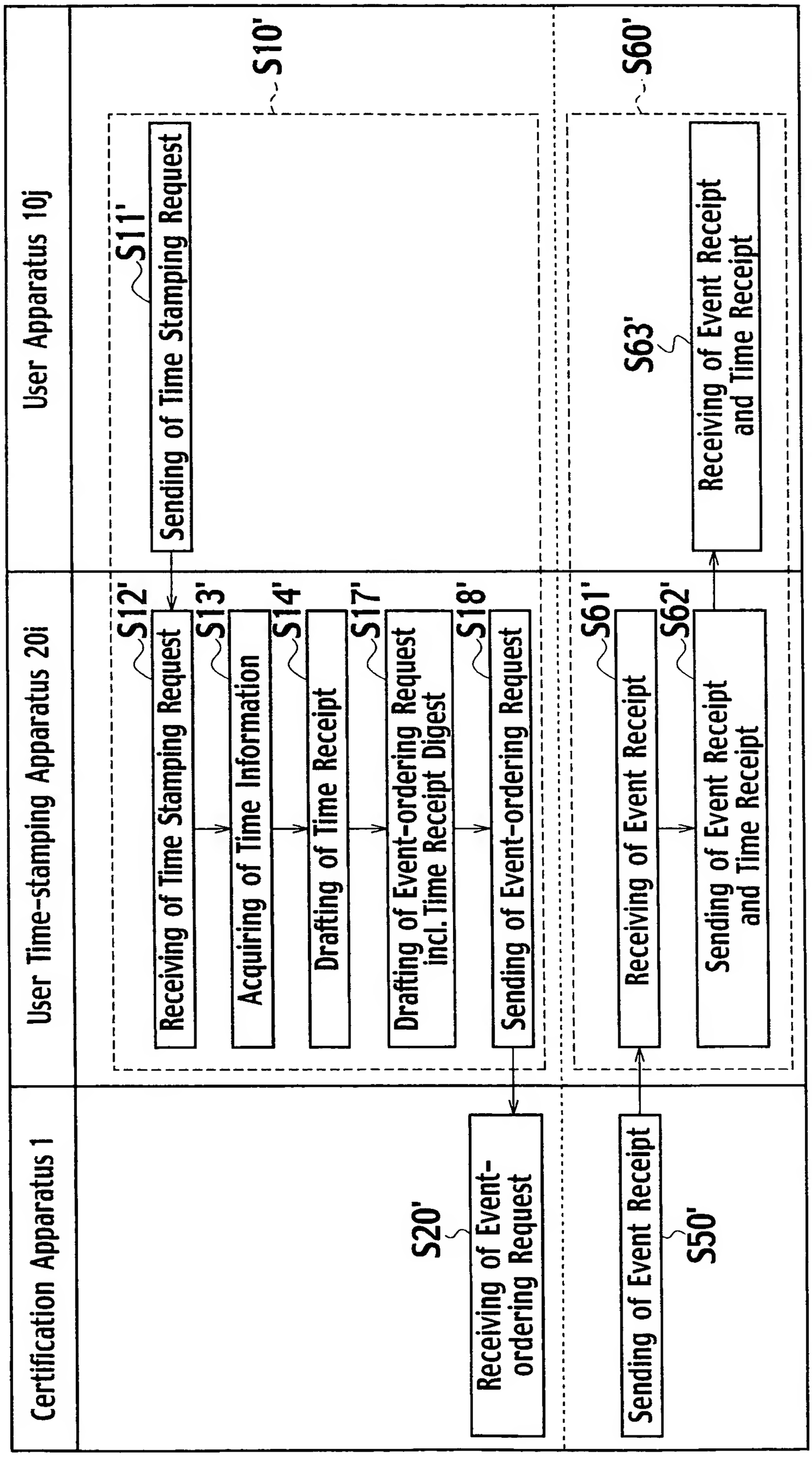

User Apparatus 10j
Time-stamping Apparatus 20i
Certification Apparatus 1
S10'
S11'
Sending of Time Stamping Request
S12'
Receiving of Time Stamping Request
S13'
Acquiring of Time Information
S14'
Drafting of Time Receipt
S17'
Drafting of Event-ordering Request incl. Time Receipt Digest
S18'
Sending of Event-ordering Request
S20'
Receiving of Event-ordering Request
S60'
S63'
Receiving of Event Receipt and Time Receipt
S61'
Receiving of Event Receipt
S62'
Sending of Event Receipt and Time Receipt
S50'
Sending of Event Receipt

FIG. 24

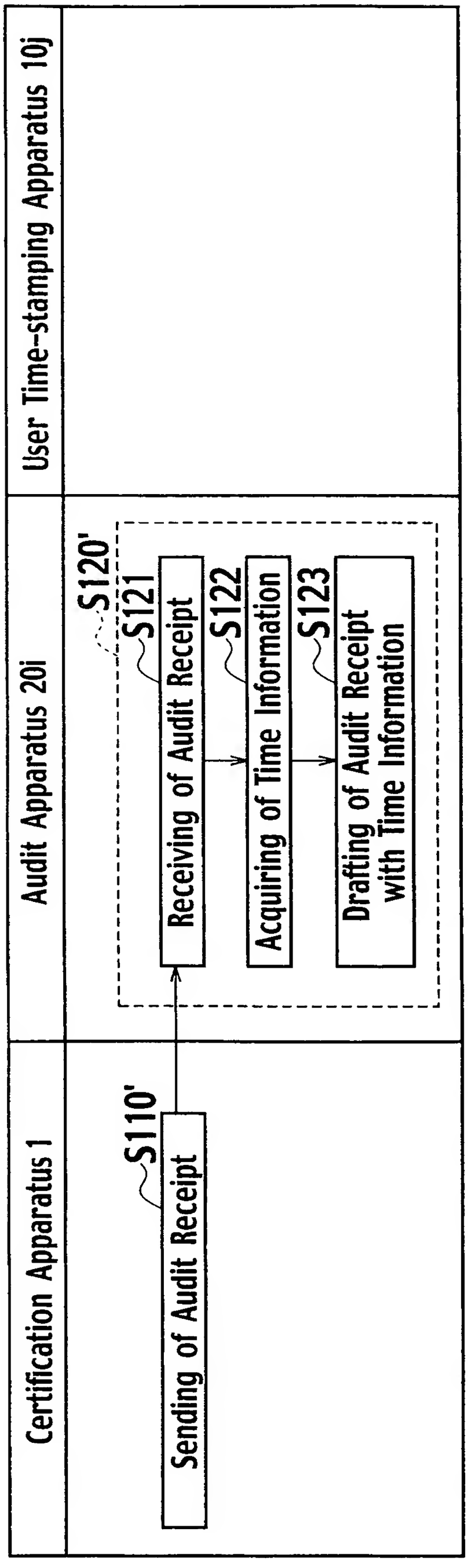

Time-stamping Apparatus 10j
User Tim
Audit Apparatus 20i
S120'
S121
Receiving of Audit Receipt
S122
Acquiring of Time Information
S123
Drafting of Audit Receipt with Time Information
Certification Apparatus 1
S110'
Sending of Audit Receipt

FIG. 25

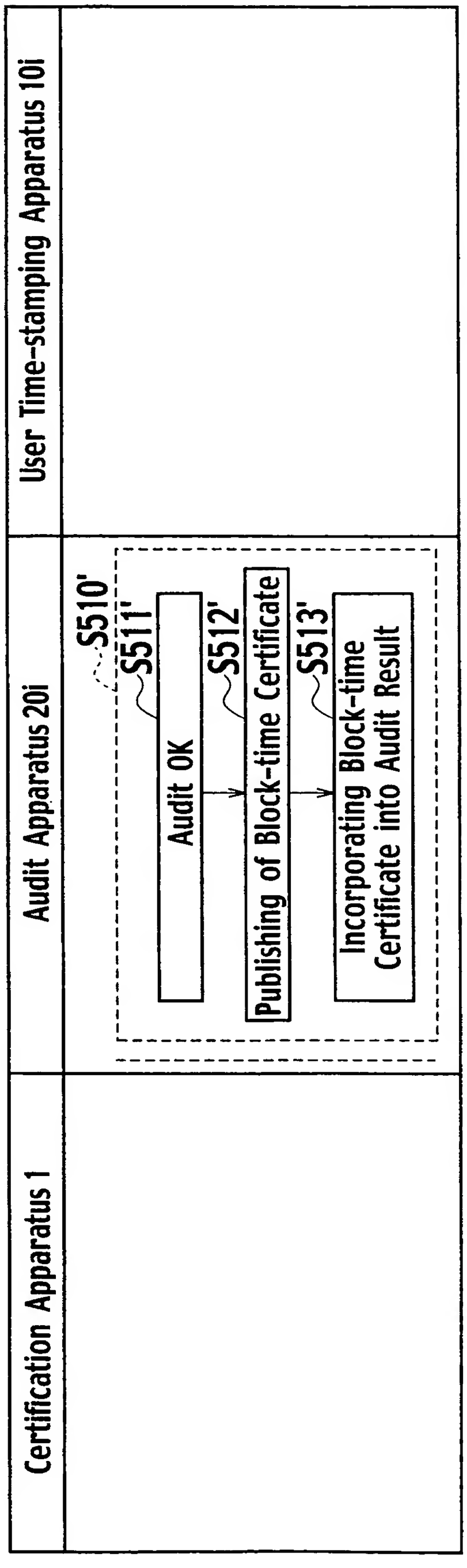

User Time-stamping Apparatus 10i
Audit Apparatus 20i
S510'
S511'
Audit OK
S512'
Publishing of Block-time Certificate
S513'
Incorporating Block-time Certificate into Audit Result
Certification Apparatus 1

FIG. 26

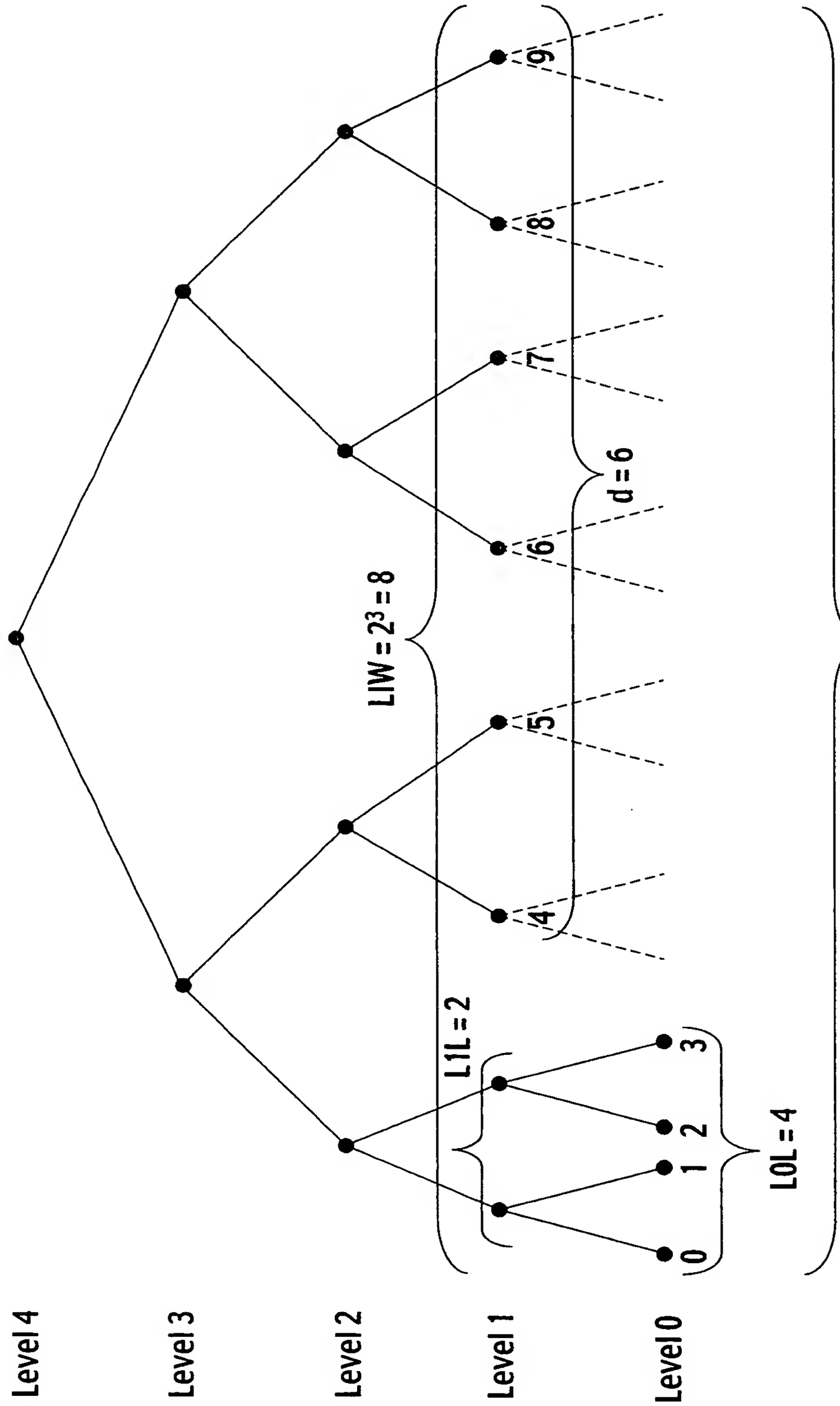

Level 4
Level 3
Level 2
Level 1
Level 0
0
1
2
3
4
5
6
7
8
9
L0L = 4
L1L = 2
LIW = 2³ = 8
d = 6
n = 10

FIG. 27

(1) Loop 1: In a constructive method No. 3, the following processes are repeated until a regular time interval is completed.

(1.1) Setting a request on acceptance to x

(1.2) Increasing n by increment of 1

(1.3) Loop 2: Performing of the follow processes for j=0, ..., k

(1.3.1) $i \rightarrow i_j$

(1.3.2) When $j = 0$, set $A_j[i] := x$.
(Set x to node(j, i_j).)

(1.3.3) When $j > 0$, perform as follows.

- Set $x0 := A_{j-1}[index(leftChiild\ (j, i))]$
(Set x0 to an assigned value for left-child of node(j, i).)
- Set $x1 := A_{j-1}[index(rightChild\ (j, i))]$
(Set x1 to an assigned value for right-child of node(j, i).)
- Calculate $x2 := h(x0 \| x1)$
- Set $A_j[i] := x2$
(Assign x2 to node(j, i).)

(1.3.4) Increasing i_j by increment of 1

(1.3.5) Withdraw from loop 2 if i is an even number.

Completion of loop 2

Completion of loop 1

Processing Procedure 1

Inventors: Fürbi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/33286
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 25 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 26 of 77

FIG. 28

(2) Performing of the following processes after withdrawing from loop 1 on reaching finish time.

(2.1) Set k:= ceiling($\log_2(n)$).

(2.2) Calculate rtPath(k, 0, n-1) and Set ((0, r(0), ..., k(, r(k))) to the calculation result.

(2.3) Loop 3:Performing of the follow processes for j=0, ..., k

(2.3.1) $i \rightarrow i_j$

(2.3.2) Case of j = 0:

(2.3.2.1) When i is an odd number:

· Produce a dummy r: = R(0, i)

· Set $A_j[i]$: = r

(Assign r to node(0, i).)

· Set b_j: = true.

· Increase i_j by increment of 1.

(2.3.2) Case of $0 < j \leqq k$:

(2.3.2.1) When i = r(j):

(when node(j, i) is on rtPath(k, 0, n-1)):

(2.3.2.1.1) x0:= A_{j-1}[index(leftChild (j, i))]

(Set x0 to an assigned value for left-child of node(j, i).)

(2.3.2.1.2) x1: = A_{j-1}[index(rightChild (j, i))]

(Set x1 to an assigned value for right-child of node(j, i).)

(2.3.2.1.3) Calculate x2: = h(x0 || x1)

(2.3.2.1.4) Set $A_j[i]$: = x2

(Assign x2 to node(j, i).)

(2.3.2.1.5) When i is an even number and j < k:

· Increase i by increment of 1.

· Calculate r: = R(j, i) and Set $A_j[i]$: = r

(Assign r to node(j, i).)

· Set b_j: = true.

· Set i_j : = i + 1

(2.3.2.2) When i = r(j) + 1, an odd number and j < k:

· Calculate r: = R(j, i) and Set $A_j[i]$: = r

(Assign r to node(j, i).)

· Set b_j: = true.

· Increase i_j by increment of 1.

Completion of loop 3

Processing Procedure 2

FIG. 29

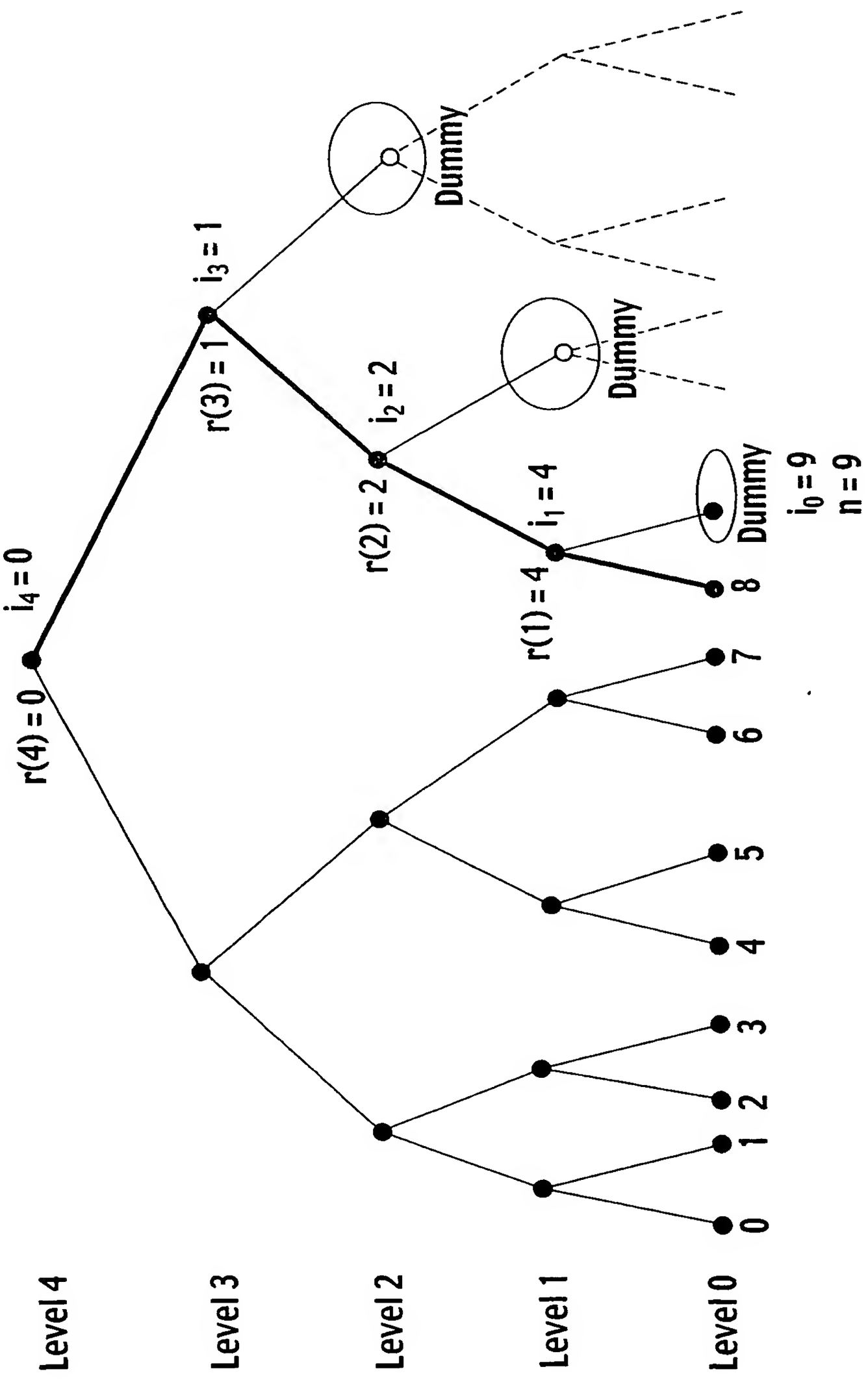
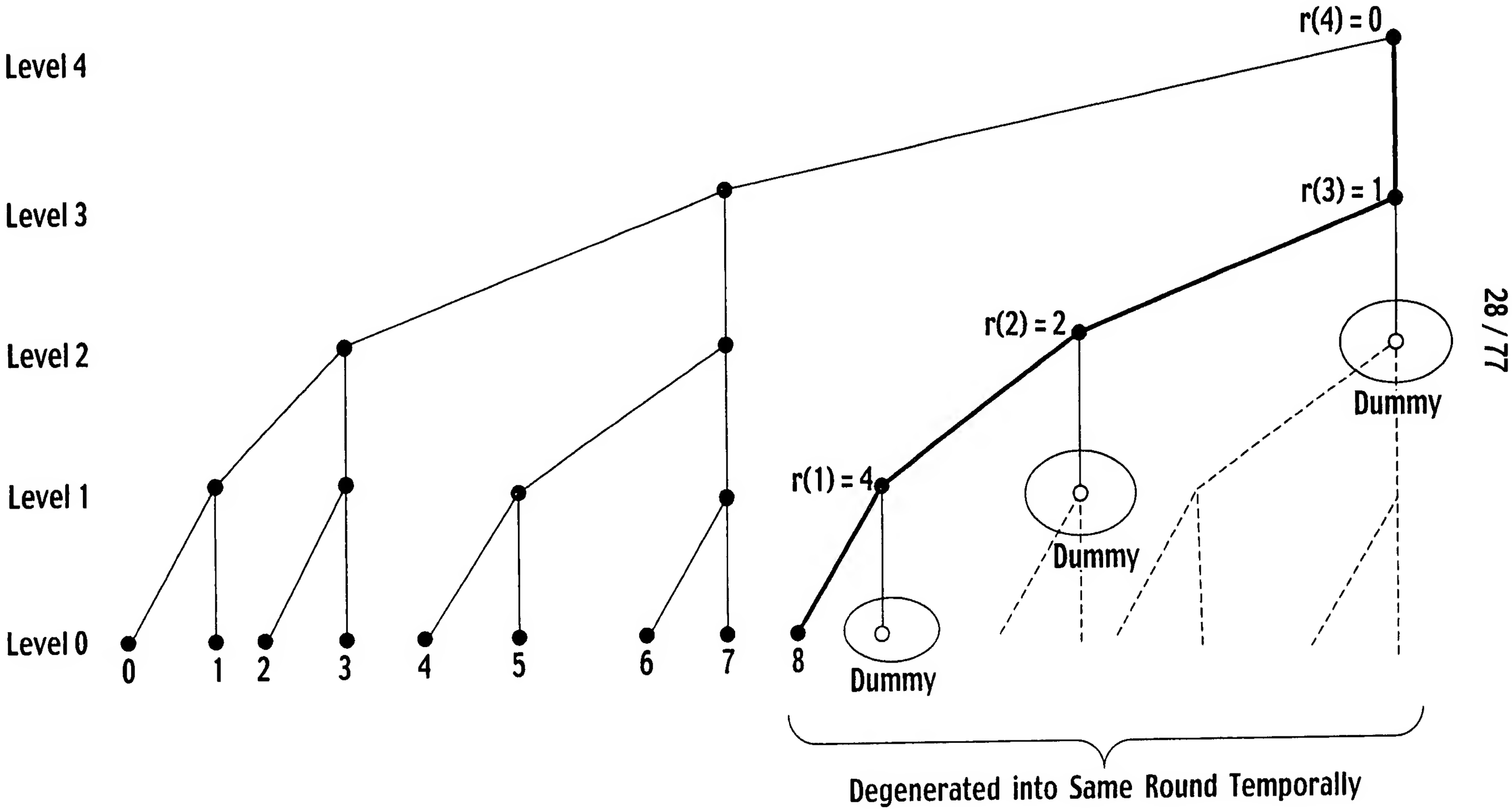

Dummy
$i_3 = 1$
$r(3) = 1$
$i_2 = 2$
$r(2) = 2$
Dummy
$i_1 = 4$
$r(1) = 4$
Dummy
$i_0 = 9$
$n = 9$
$i_4 = 0$
$r(4) = 0$
8
7
6
5
4
3
2
1
0
Level 4
Level 3
Level 2
Level 1
Level 0

FIG. 30



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 28 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 29 of 77

FIG. 31

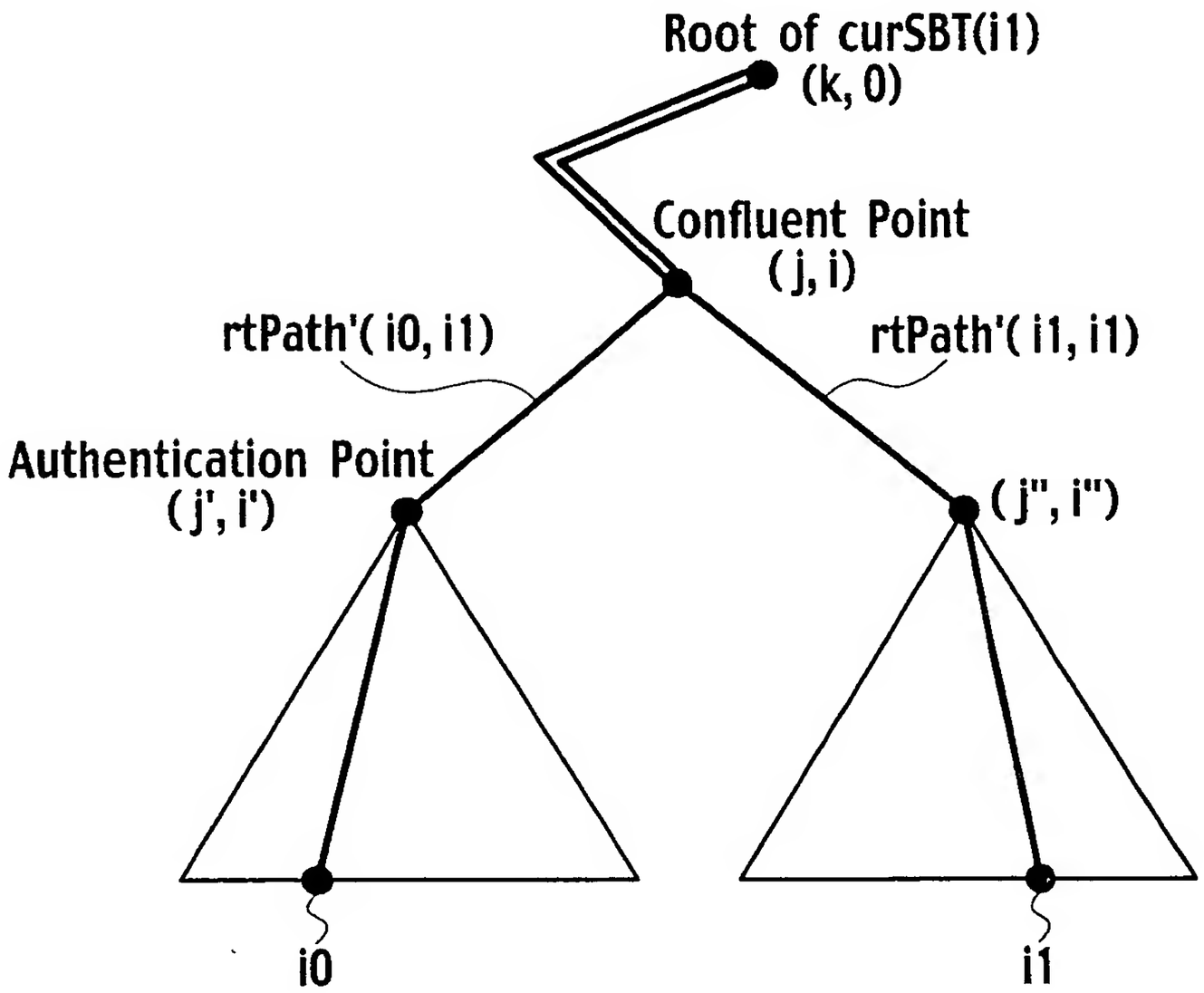


FIG. 32

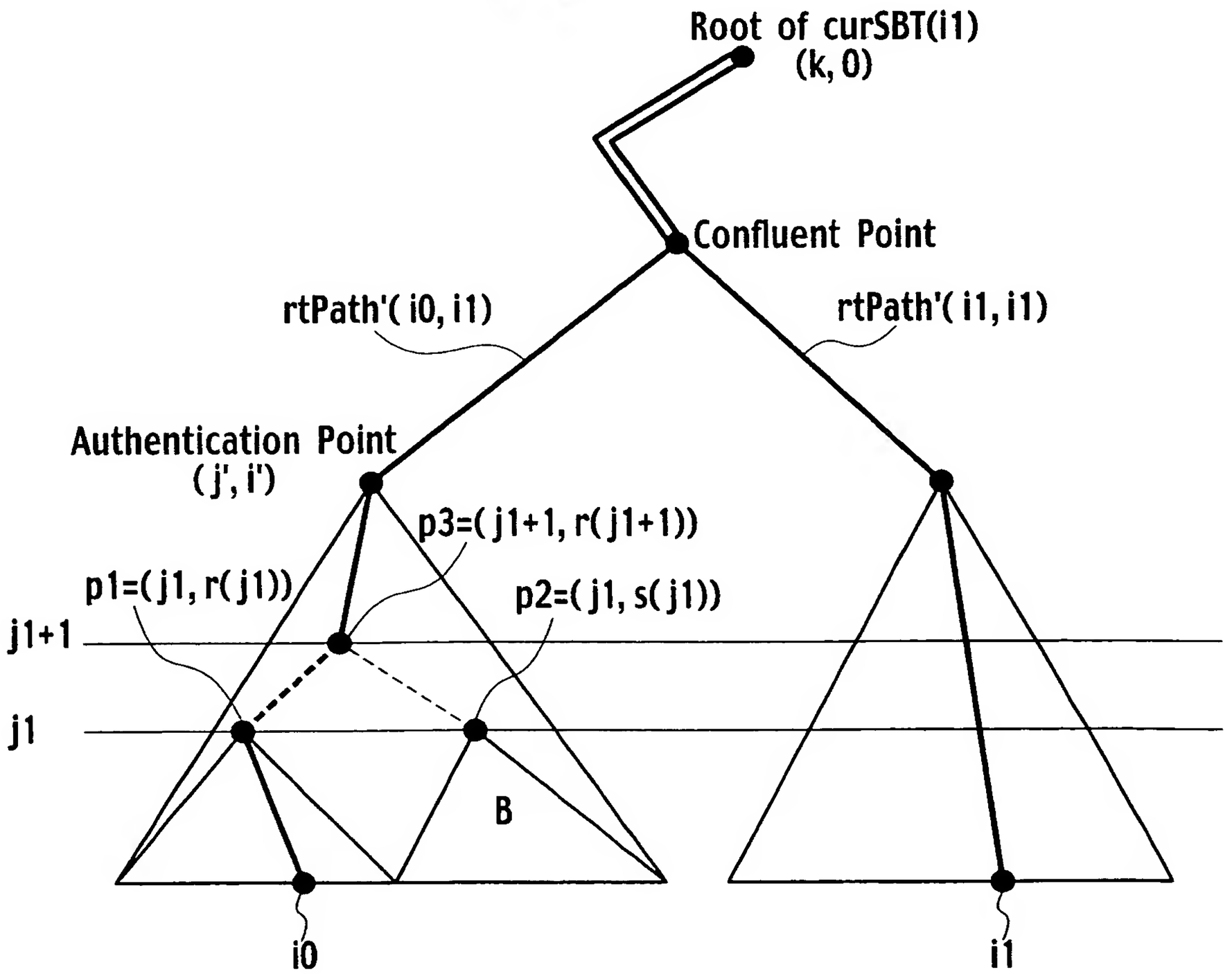


FIG. 33

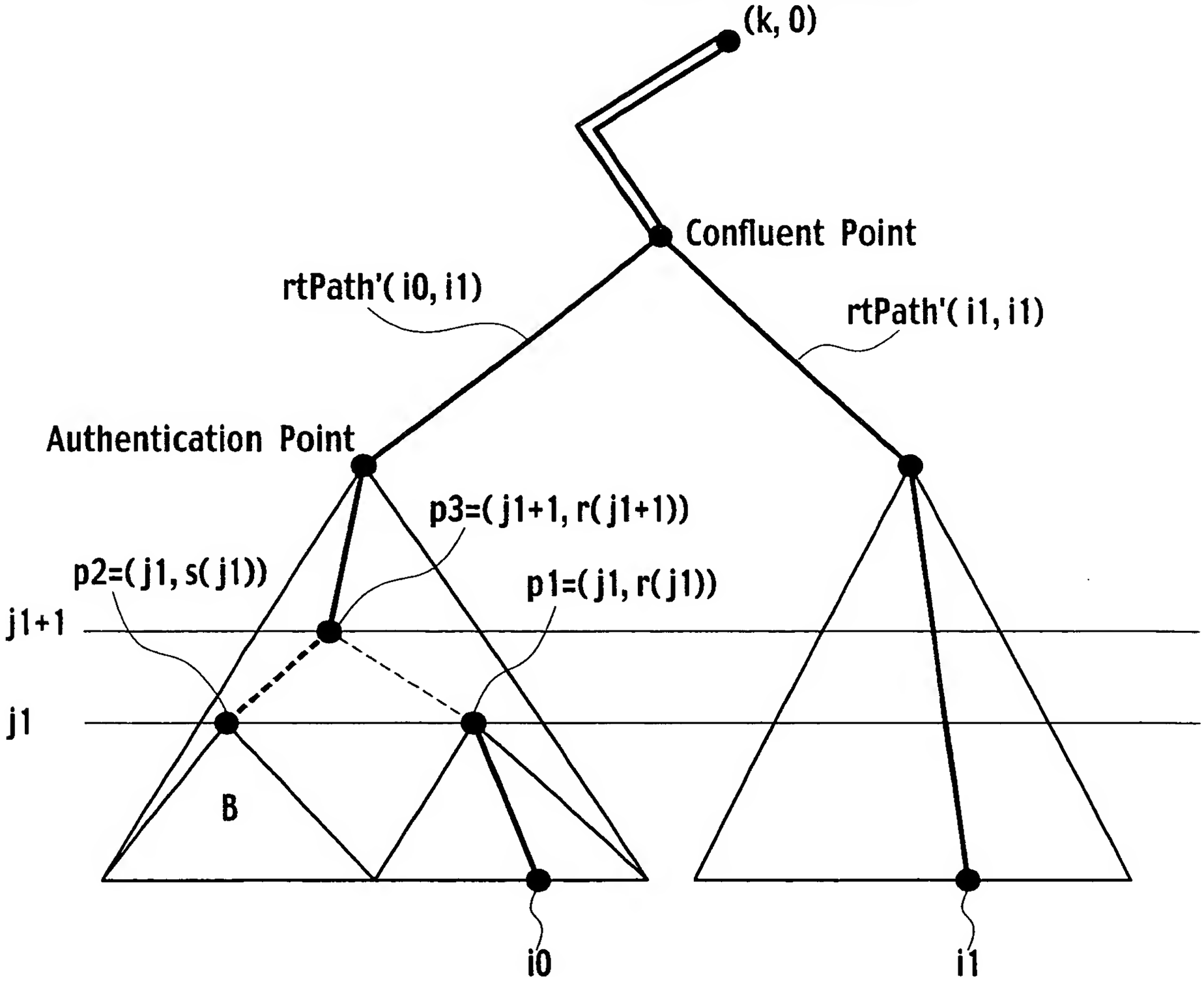

Root of curSBT(i1)
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

FIG. 34

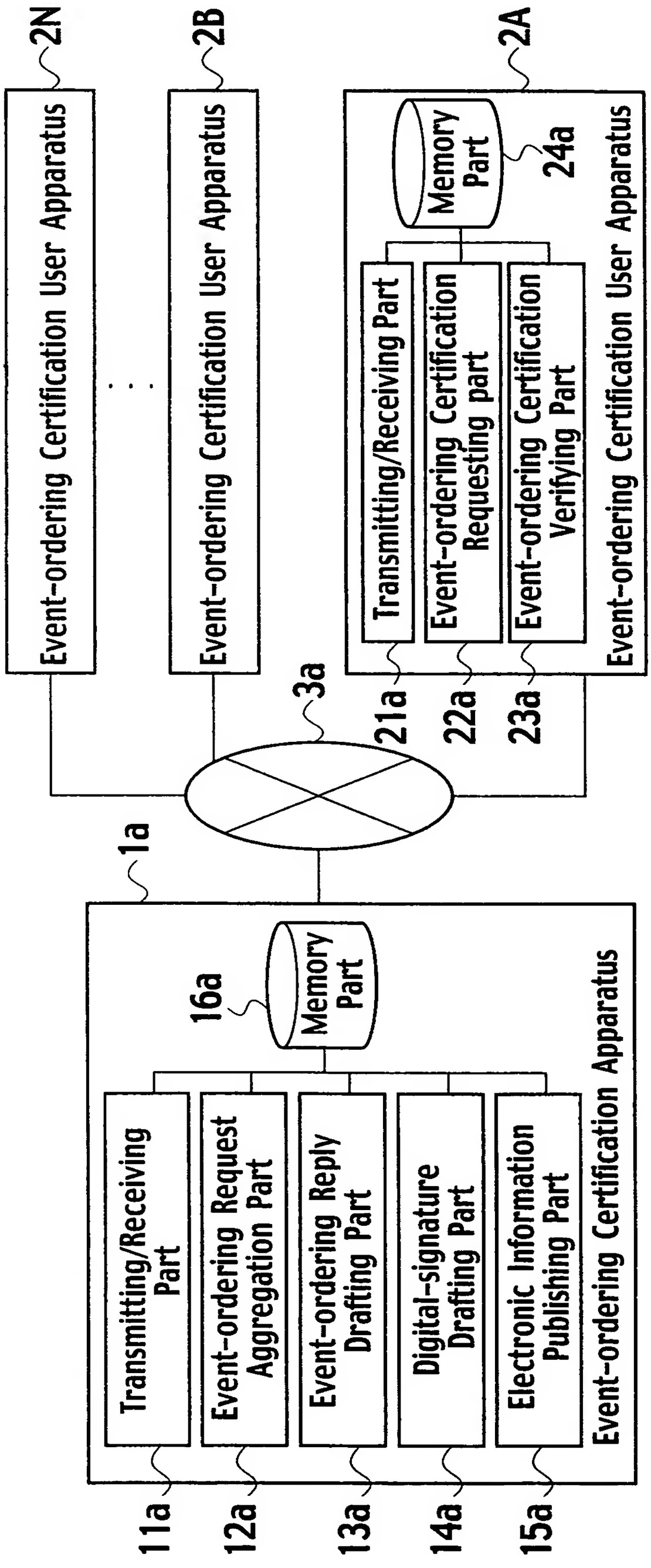
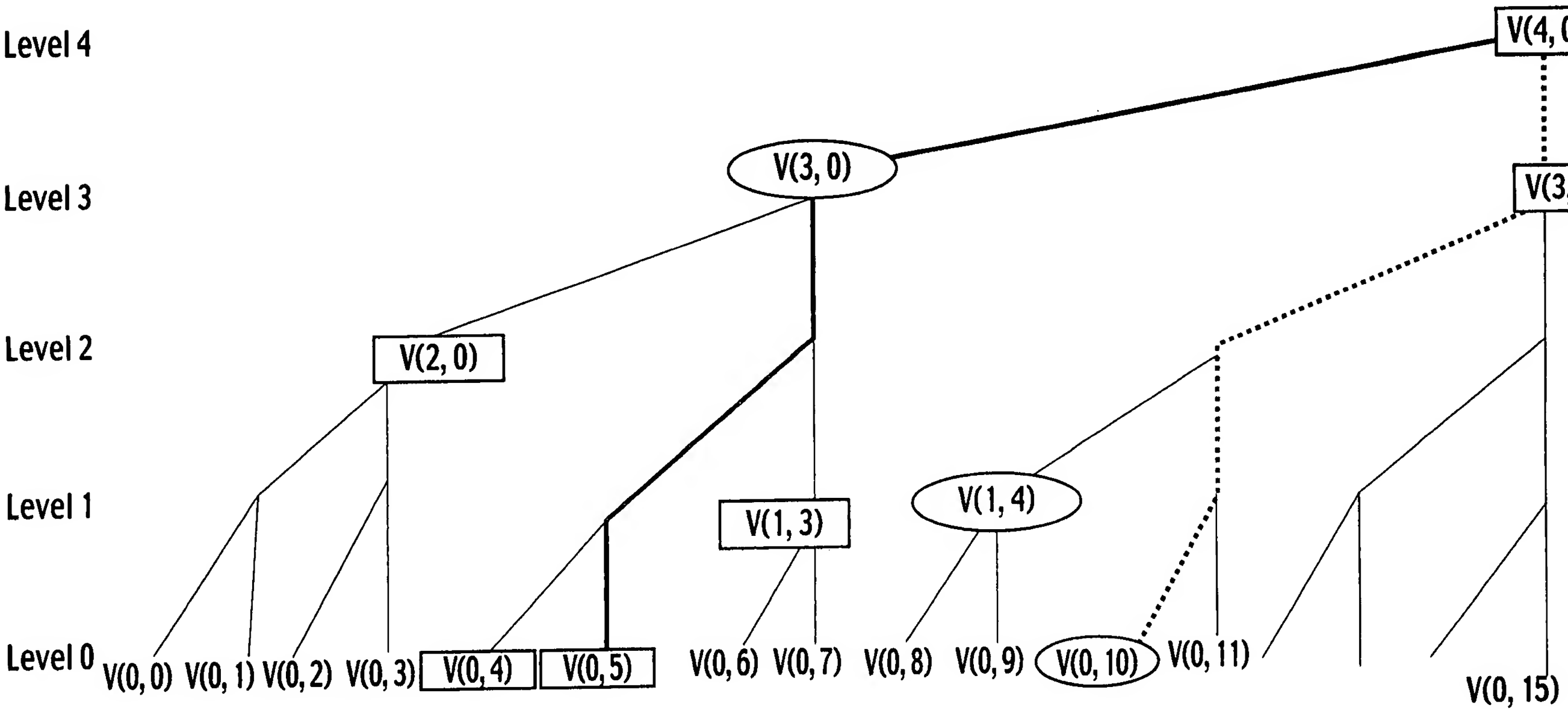

2N
2B
2A
Event-ordering Certification User Apparatus
Event-ordering Certification User Apparatus
Event-ordering Certification User Apparatus
Memory Part
24a
Transmitting/Receiving Part
Event-ordering Certification Requesting part
Event-ordering Certification Verifying Part
3a
21a
22a
23a
1a
16a
Memory Part
Transmitting/Receiving Part
Event-ordering Request Aggregation Part
Event-ordering Reply Drafting Part
Digital-signature Drafting Part
Electronic Information Publishing Part
Event-ordering Certification Apparatus
11a
12a
13a
14a
15a
100a

FIG. 35



Inventors: Eitan HORVITZ
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500

FIG. 36

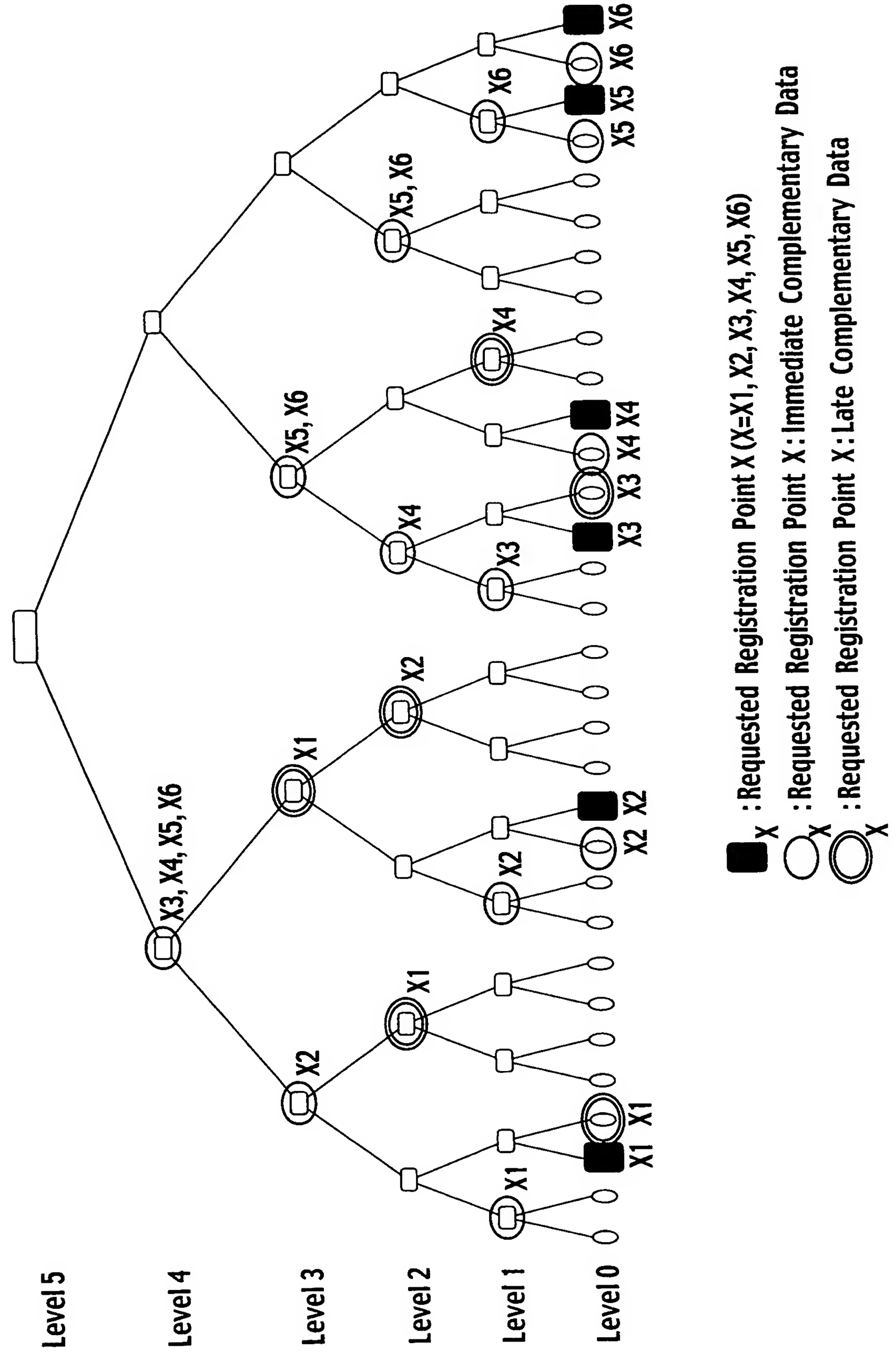
ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○
Late Complementary Data of Each Past Registration Point (Positional Information Assigned Value)	TK	○

Event-ordering Receipt EOC(y)

Inventors: Eiichi HOSOYA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 33 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 34 of 77

FIG. 37



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 35 of 77

FIG. 38

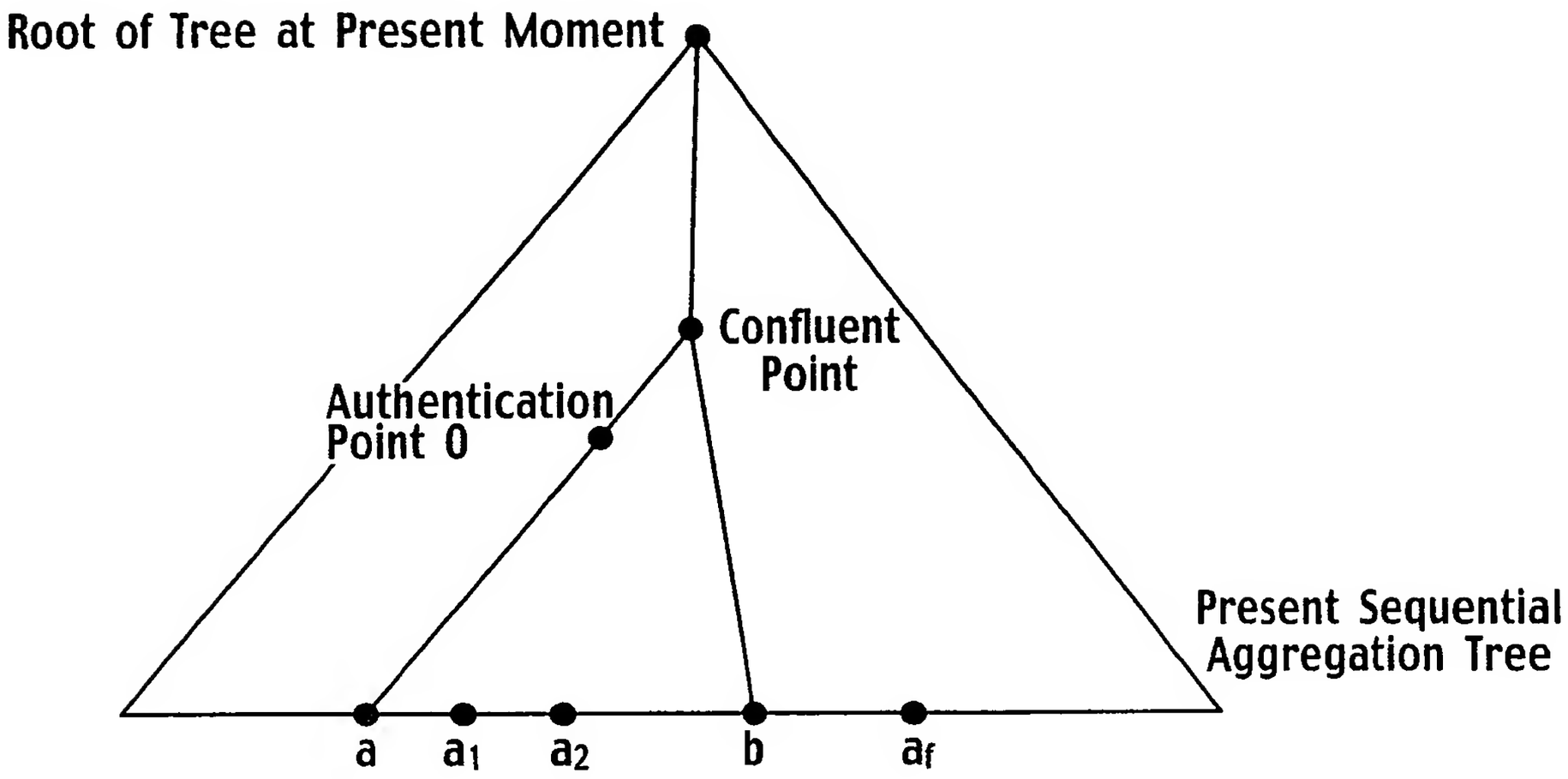


FIG. 39

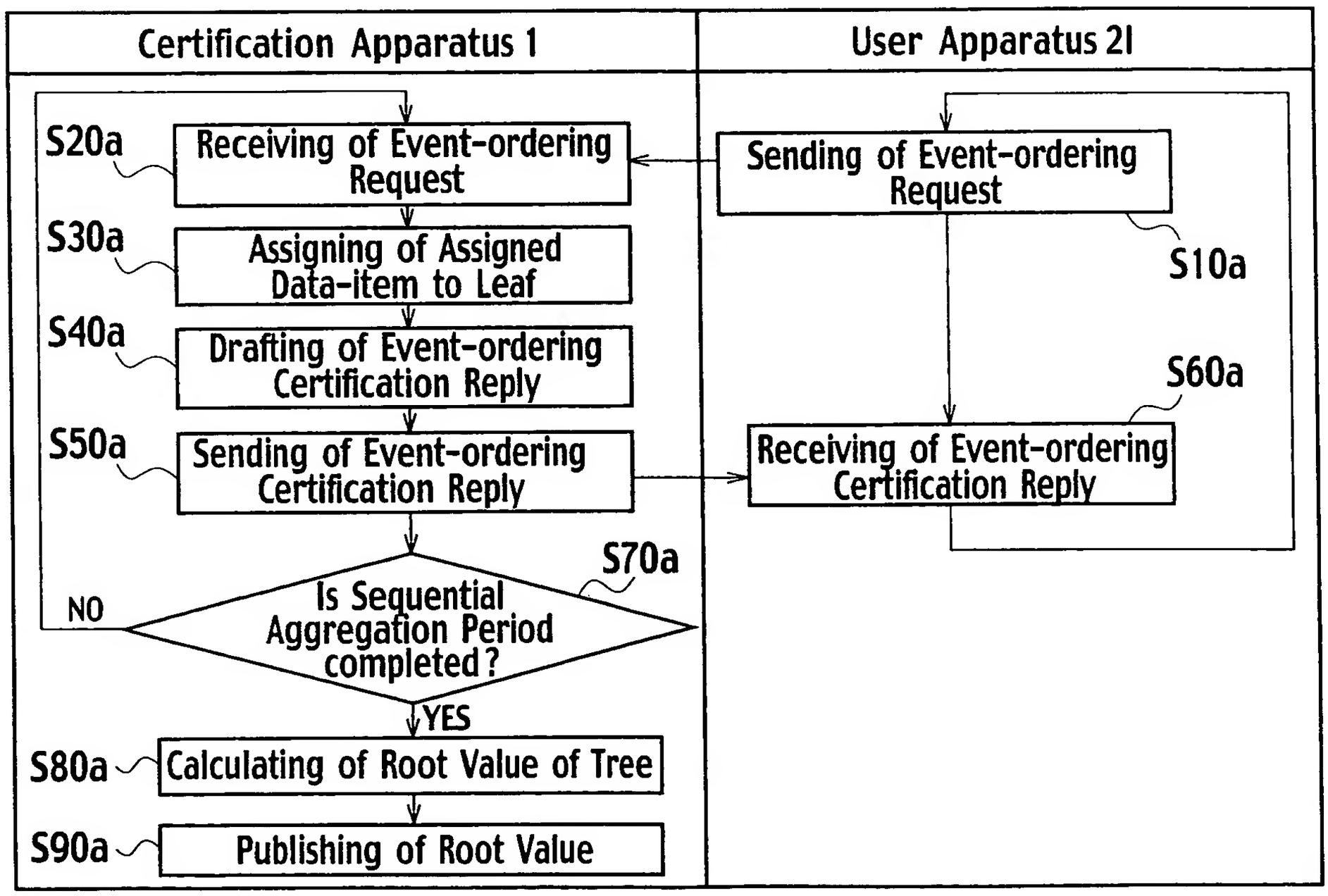


FIG. 40

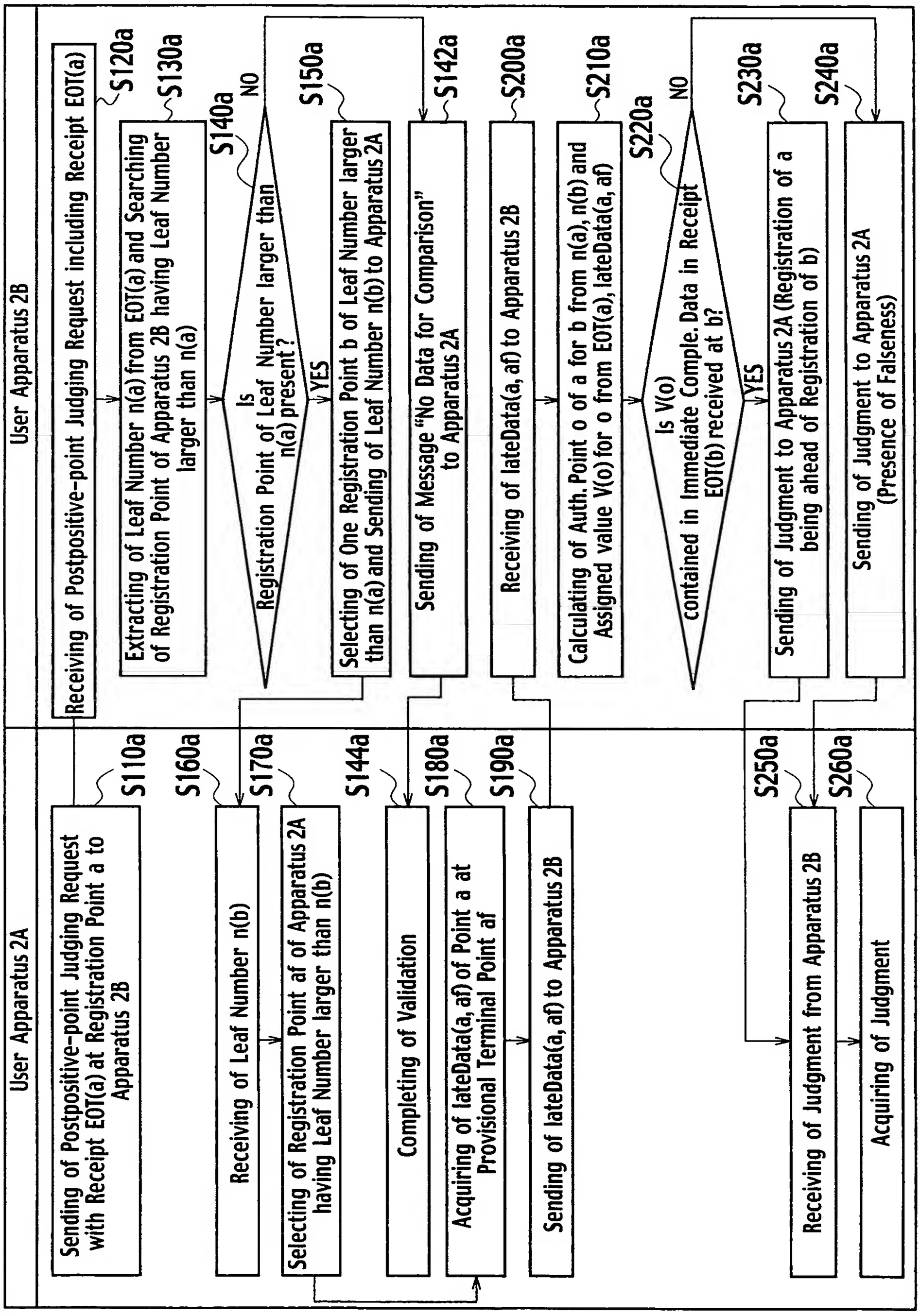
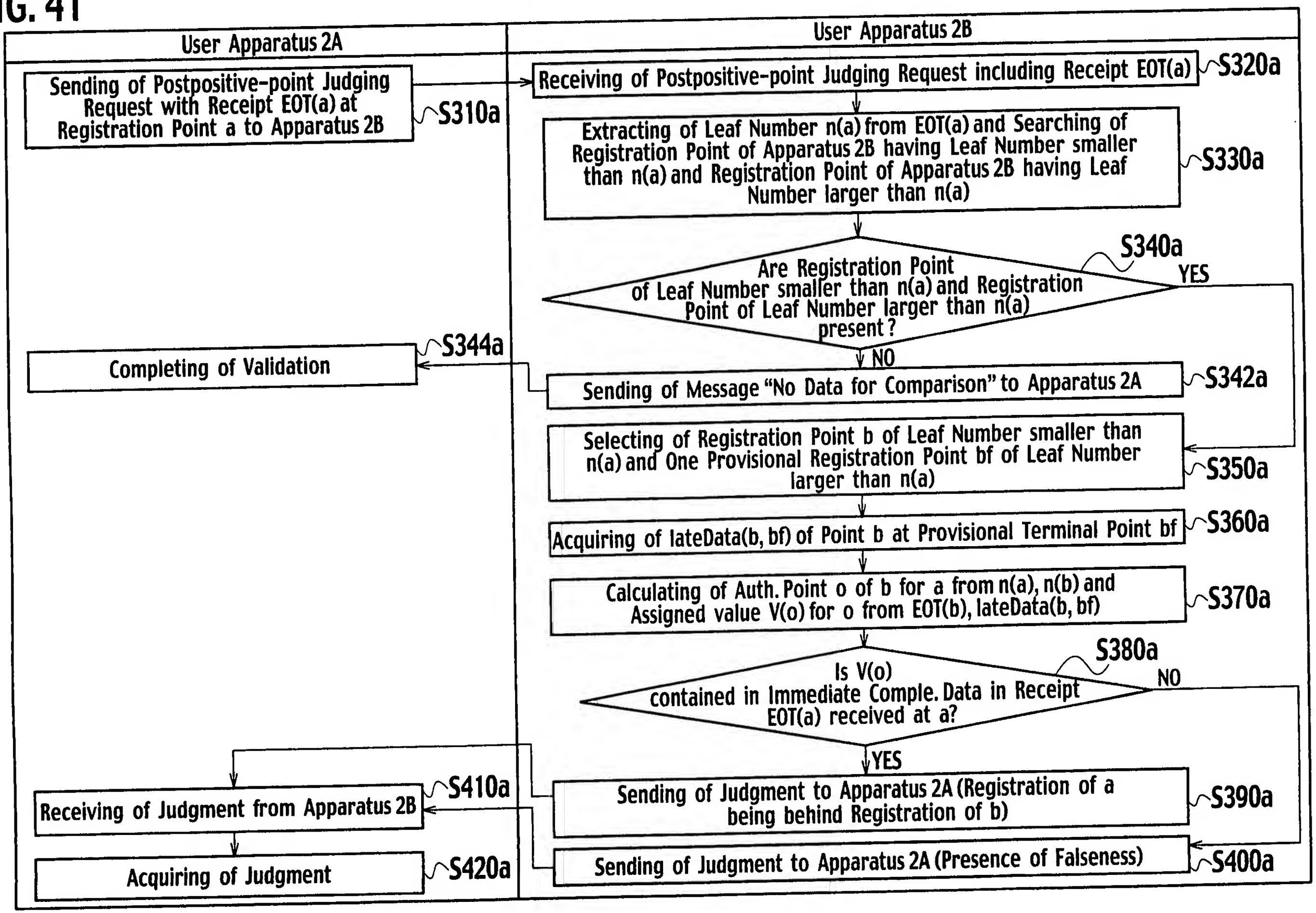

User Apparatus 2B
Receiving of Postpositive-point Judging Request including Receipt EOT(a)
S120a
Extracting of Leaf Number n(a) from EOT(a) and Searching of Registration Point of Apparatus 2B having Leaf Number larger than n(a)
S130a
S140a
NO
Is Registration Point of Leaf Number n(a) present?
YES
S150a
Selecting of One Registration Point b of Leaf Number larger than n(a) and Sending of Leaf Number n(b) to Apparatus 2A
S142a
Sending of Message "No Data for Comparison" to Apparatus 2A
S200a
Receiving of lateData(a, af) to Apparatus 2B
S210a
Calculating of Auth. Point o of a for b from n(a), n(b) and Assigned value V(o) for o from EOT(a), lateData(a, af)
S220a
NO
Is V(o) contained in Immediate Comple. Data in Receipt EOT(b) received at b?
YES
S230a
Sending of Judgment to Apparatus 2A (Registration of a being ahead of Registration of b)
S240a
Sending of Judgment to Apparatus 2A (Presence of Falseness)
User Apparatus 2A
S110a
Sending of Postpositive-point Judging Request with Receipt EOT(a) at Registration Point a to Apparatus 2B
S160a
Receiving of Leaf Number n(b)
S170a
Selecting of Registration Point af of Apparatus 2A having Leaf Number larger than n(b)
S144a
Completing of Validation
S180a
Acquiring of lateData(a, af) of Point a at Provisional Terminal Point af
S190a
Sending of lateData(a, af) to Apparatus 2B
S250a
Receiving of Judgment from Apparatus 2B
S260a
Acquiring of Judgment

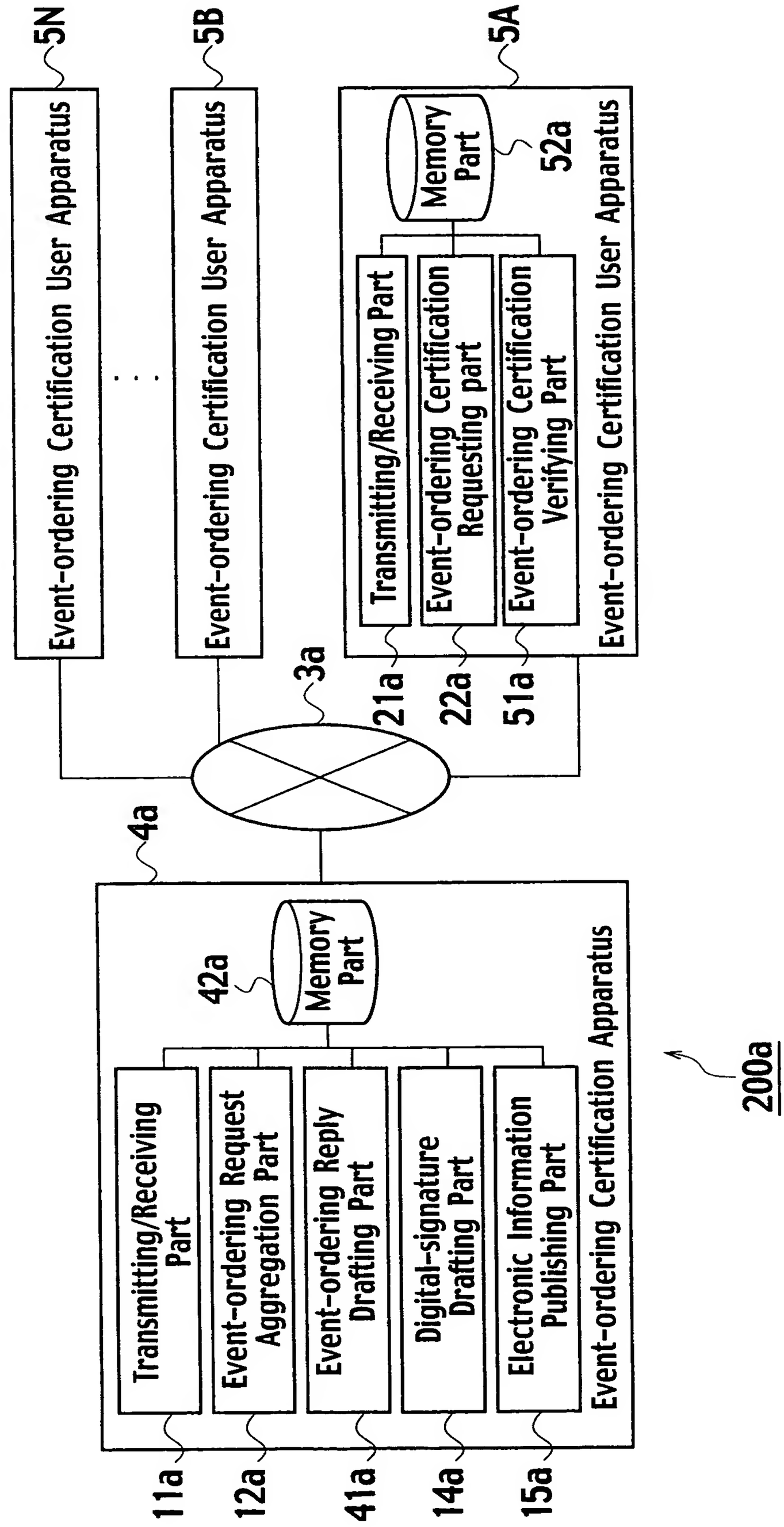
FIG. 41



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4447I/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 37 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 38 of 77

FIG. 42



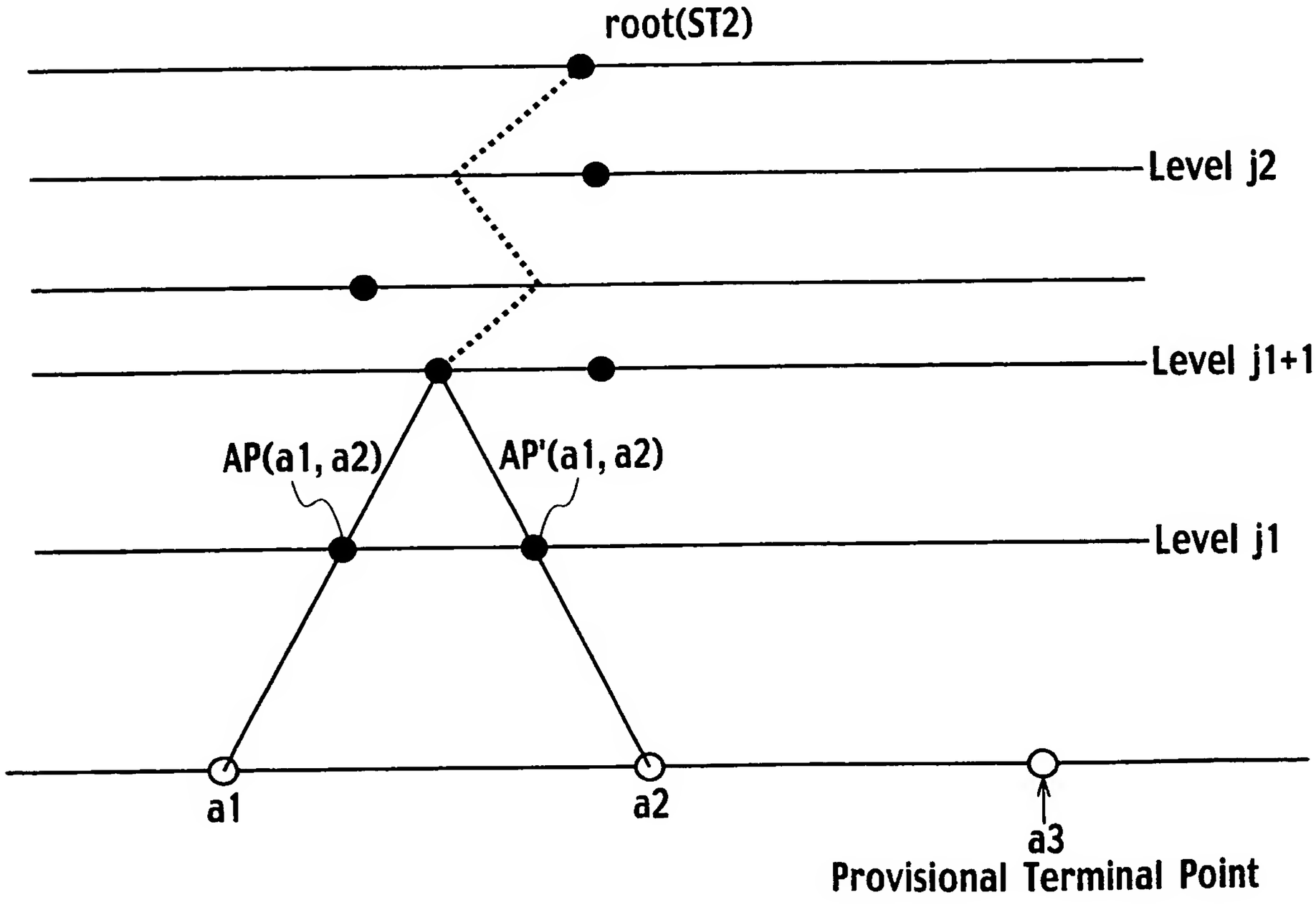
Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 39 of 77

FIG. 43

ITEM	SIGN	REQUIRED
Original Data	y	○
Sequentially Assigned Data-item	z	○
Sequential Aggregation Tree No.	n	○
Sequential Aggregation Tree Leaf No.	i	○
Immediate Complementary Data of Registration Point (Positional Information Assigned Value)	SK	○
Late Complementary Data of Immediately-preceding Registration Point (Positional Information Assigned Value)	TK2	○

Event-ordering Receipt EOC(y)

FIG. 44



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 40 of 77

FIG. 45

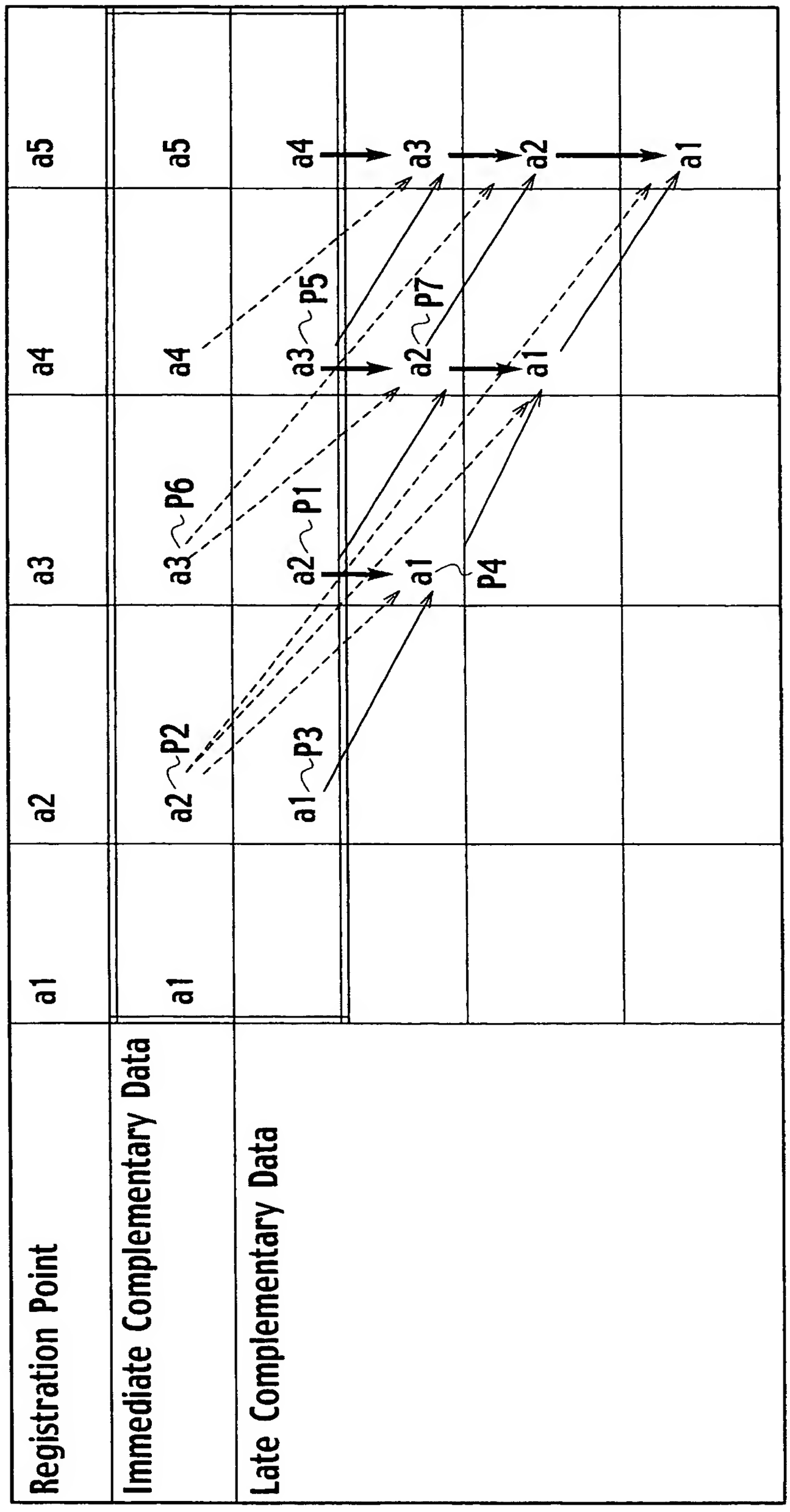
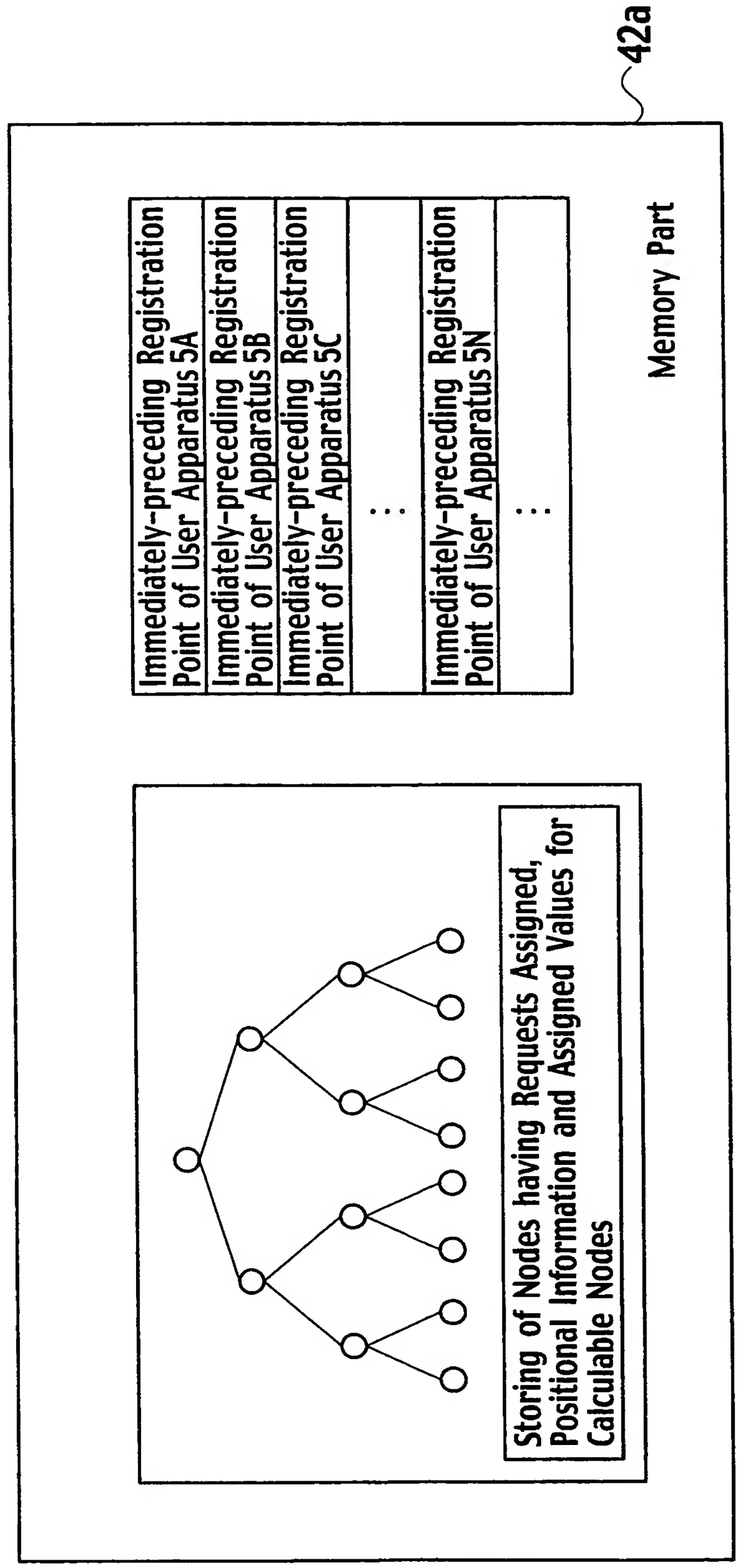


FIG. 46


42a
Memory Part
Immediately-preceding Registration Point of User Apparatus 5A
Immediately-preceding Registration Point of User Apparatus 5B
Immediately-preceding Registration Point of User Apparatus 5C
Immediately-preceding Registration Point of User Apparatus 5N
Storing of Nodes having Requests Assigned, Positional Information and Assigned Values for Calculable Nodes

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 42 of 77

FIG. 47

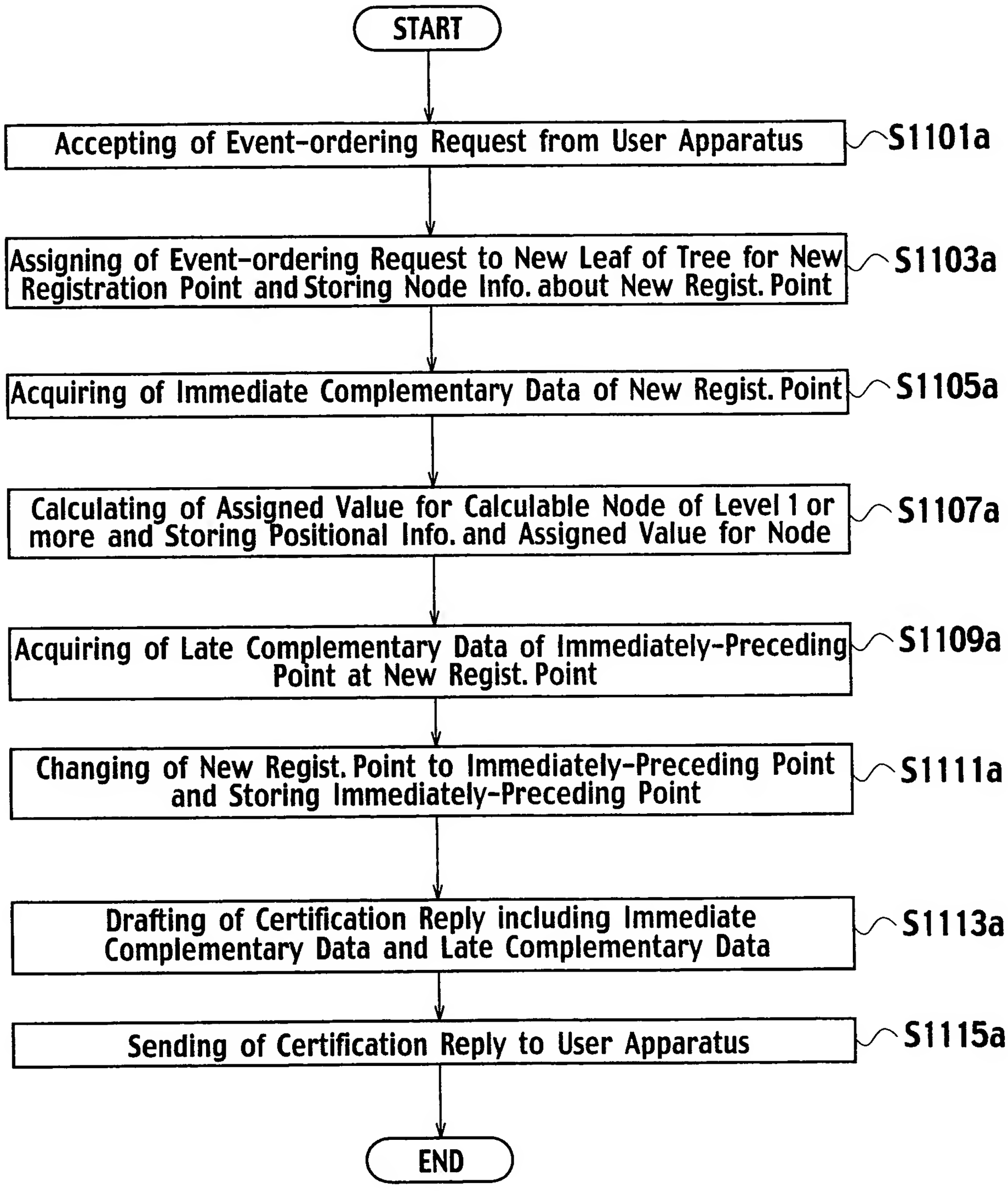
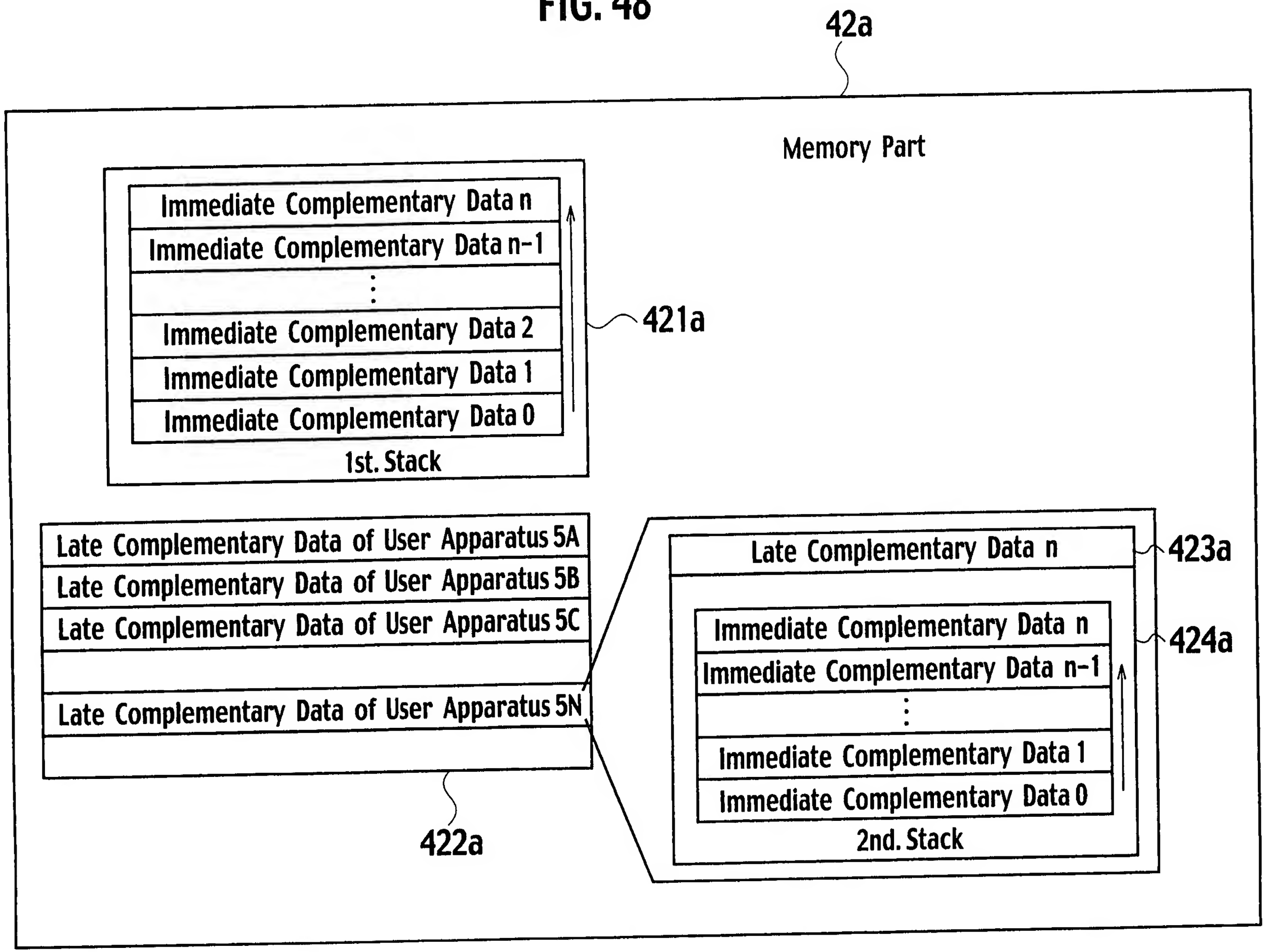


FIG. 48



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 4471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 43 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 44 of 77

FIG. 49

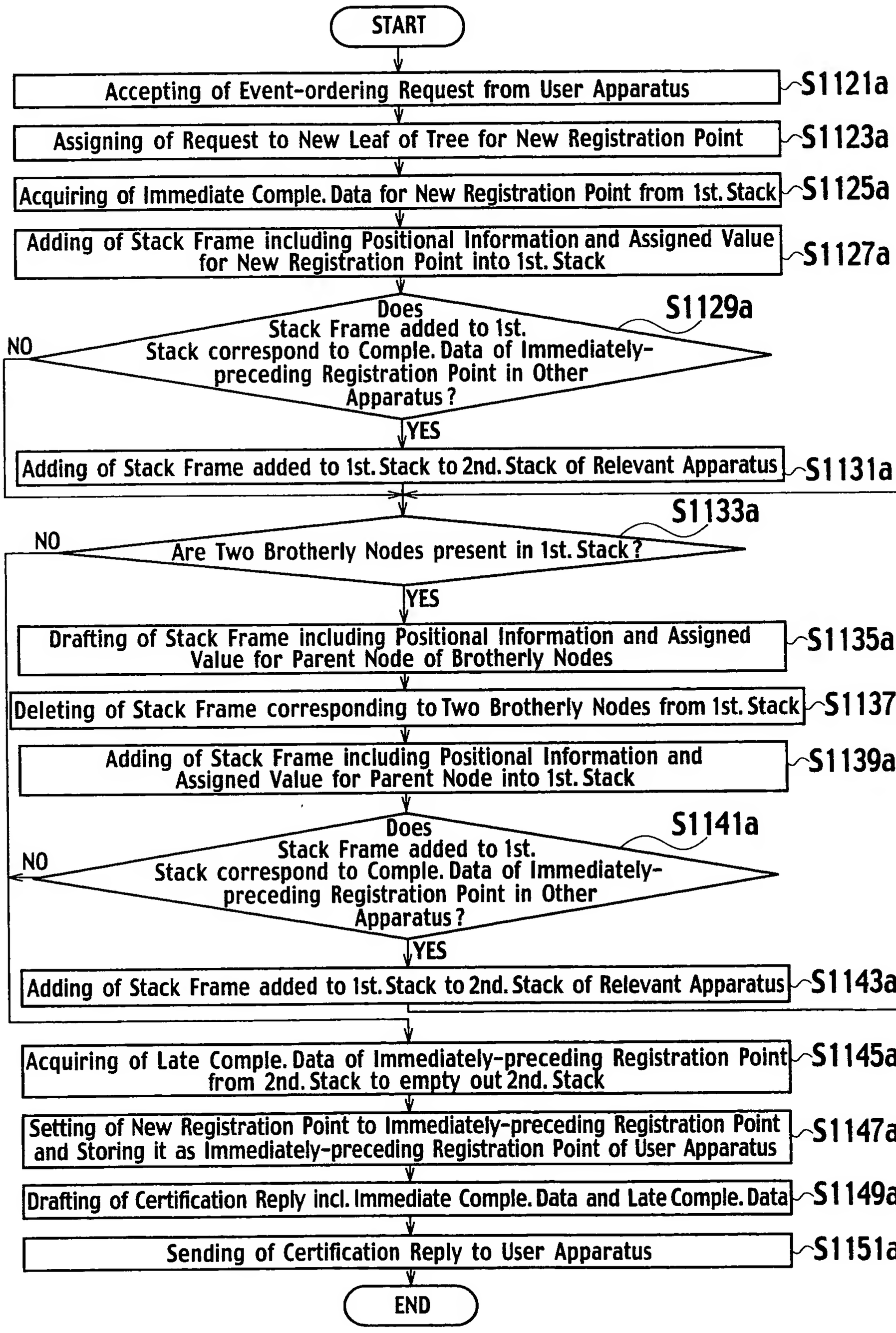


FIG. 50

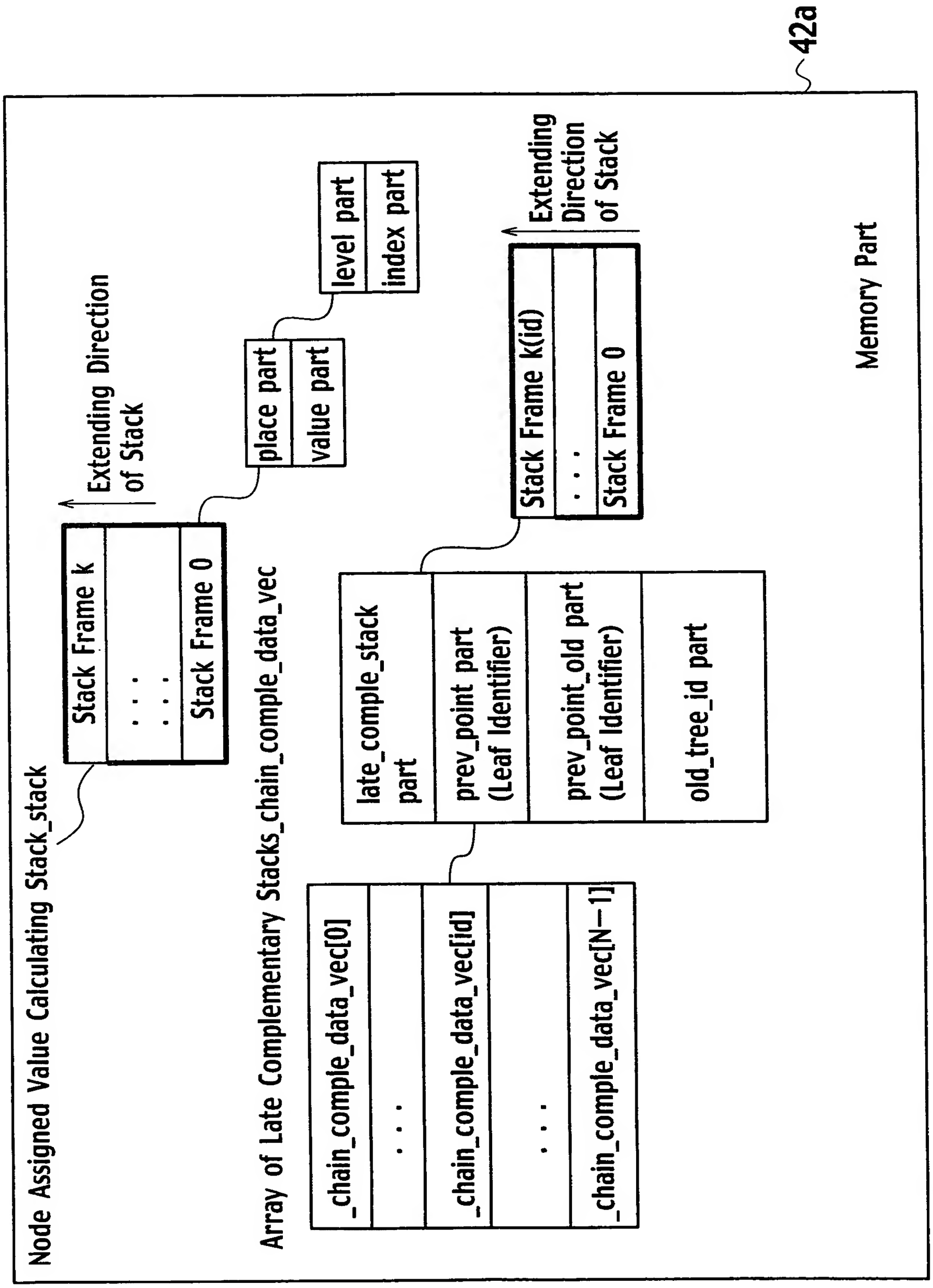

42a
Node Assigned Value Calculating Stack_stack
Stack Frame k
. . .
. . .
Stack Frame 0
Extending Direction of Stack
level part
index part
place part
value part
Array of Late Complementary Stacks_chain_comple_data_vec
_chain_comple_data_vec[0]
. . .
_chain_comple_data_vec[id]
. . .
_chain_comple_data_vec[N−1]
late_comple_stack part
prev_point part (Leaf Identifier)
prev_point_old part (Leaf Identifier)
old_tree_id part
Extending Direction of Stack
Stack Frame k(id)
. . .
Stack Frame 0
Memory Part

FIG. 51

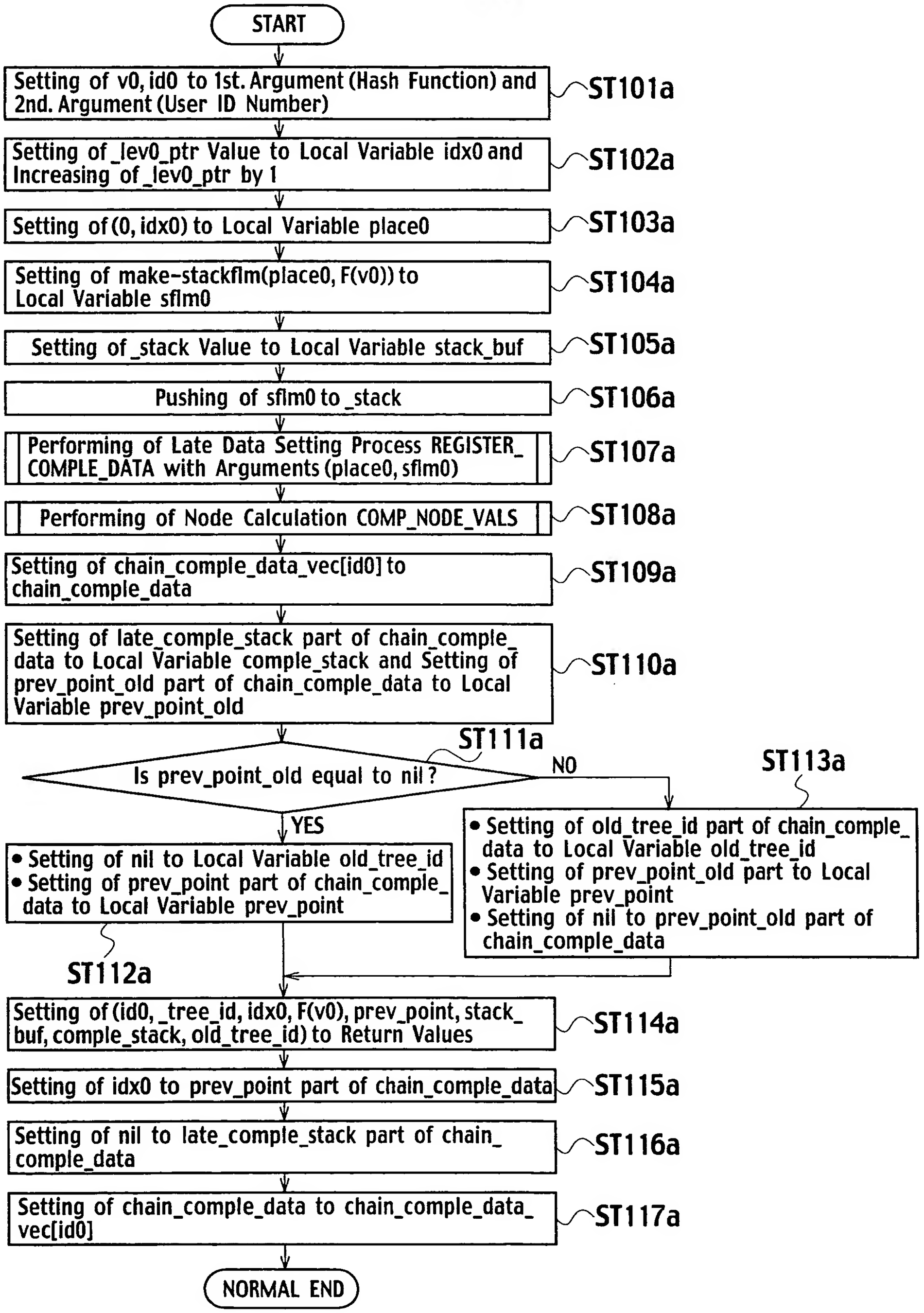

START
Setting of v0, id0 to 1st. Argument (Hash Function) and 2nd. Argument (User ID Number)
ST101a
Setting of _lev0_ptr Value to Local Variable idx0 and Increasing of _lev0_ptr by 1
ST102a
Setting of (0, idx0) to Local Variable place0
ST103a
Setting of make-stackflm(place0, F(v0)) to Local Variable sflm0
ST104a
Setting of _stack Value to Local Variable stack_buf
ST105a
Pushing of sflm0 to _stack
ST106a
Performing of Late Data Setting Process REGISTER_COMPLE_DATA with Arguments (place0, sflm0)
ST107a
Performing of Node Calculation COMP_NODE_VALS
ST108a
Setting of chain_comple_data_vec[id0] to chain_comple_data
ST109a
Setting of late_comple_stack part of chain_comple_data to Local Variable comple_stack and Setting of prev_point_old part of chain_comple_data to Local Variable prev_point_old
ST110a
ST111a
Is prev_point_old equal to nil ?
NO
ST113a
YES
• Setting of nil to Local Variable old_tree_id
• Setting of prev_point part of chain_comple_data to Local Variable prev_point
• Setting of old_tree_id part of chain_comple_data to Local Variable old_tree_id
• Setting of prev_point_old part to Local Variable prev_point
• Setting of nil to prev_point_old part of chain_comple_data
ST112a
Setting of (id0, _tree_id, idx0, F(v0), prev_point, stack_buf, comple_stack, old_tree_id) to Return Values
ST114a
Setting of idx0 to prev_point part of chain_comple_data
ST115a
Setting of nil to late_comple_stack part of chain_comple_data
ST116a
Setting of chain_comple_data to chain_comple_data_vec[id0]
ST117a
NORMAL END

FIG. 52

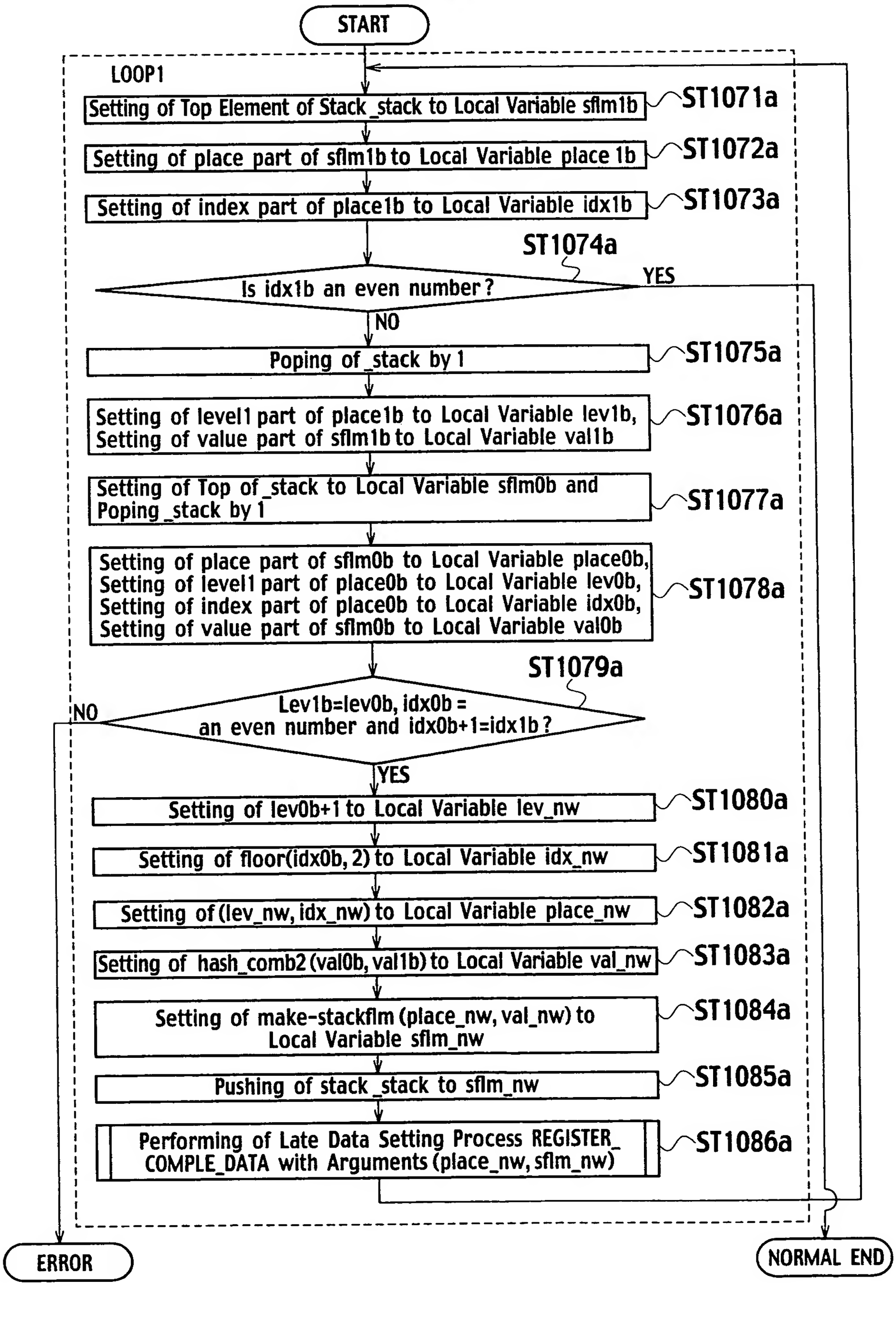

START
LOOP1
Setting of Top Element of Stack_stack to Local Variable sflm1b
ST1071a
Setting of place part of sflm1b to Local Variable place1b
ST1072a
Setting of index part of place1b to Local Variable idx1b
ST1073a
ST1074a
Is idx1b an even number?
YES
NO
Poping of_stack by 1
ST1075a
Setting of level1 part of place1b to Local Variable lev1b,
Setting of value part of sflm1b to Local Variable val1b
ST1076a
Setting of Top of_stack to Local Variable sflm0b and
Poping_stack by 1
ST1077a
Setting of place part of sflm0b to Local Variable place0b,
Setting of level1 part of place0b to Local Variable lev0b,
Setting of index part of place0b to Local Variable idx0b,
Setting of value part of sflm0b to Local Variable val0b
ST1078a
ST1079a
Lev1b=lev0b, idx0b =
an even number and idx0b+1=idx1b?
NO
YES
Setting of lev0b+1 to Local Variable lev_nw
ST1080a
Setting of floor(idx0b, 2) to Local Variable idx_nw
ST1081a
Setting of (lev_nw, idx_nw) to Local Variable place_nw
ST1082a
Setting of hash_comb2 (val0b, val1b) to Local Variable val_nw
ST1083a
Setting of make-stackflm (place_nw, val_nw) to
Local Variable sflm_nw
ST1084a
Pushing of stack_stack to sflm_nw
ST1085a
Performing of Late Data Setting Process REGISTER_
COMPLE_DATA with Arguments (place_nw, sflm_nw)
ST1086a
ERROR
NORMAL END

FIG. 53

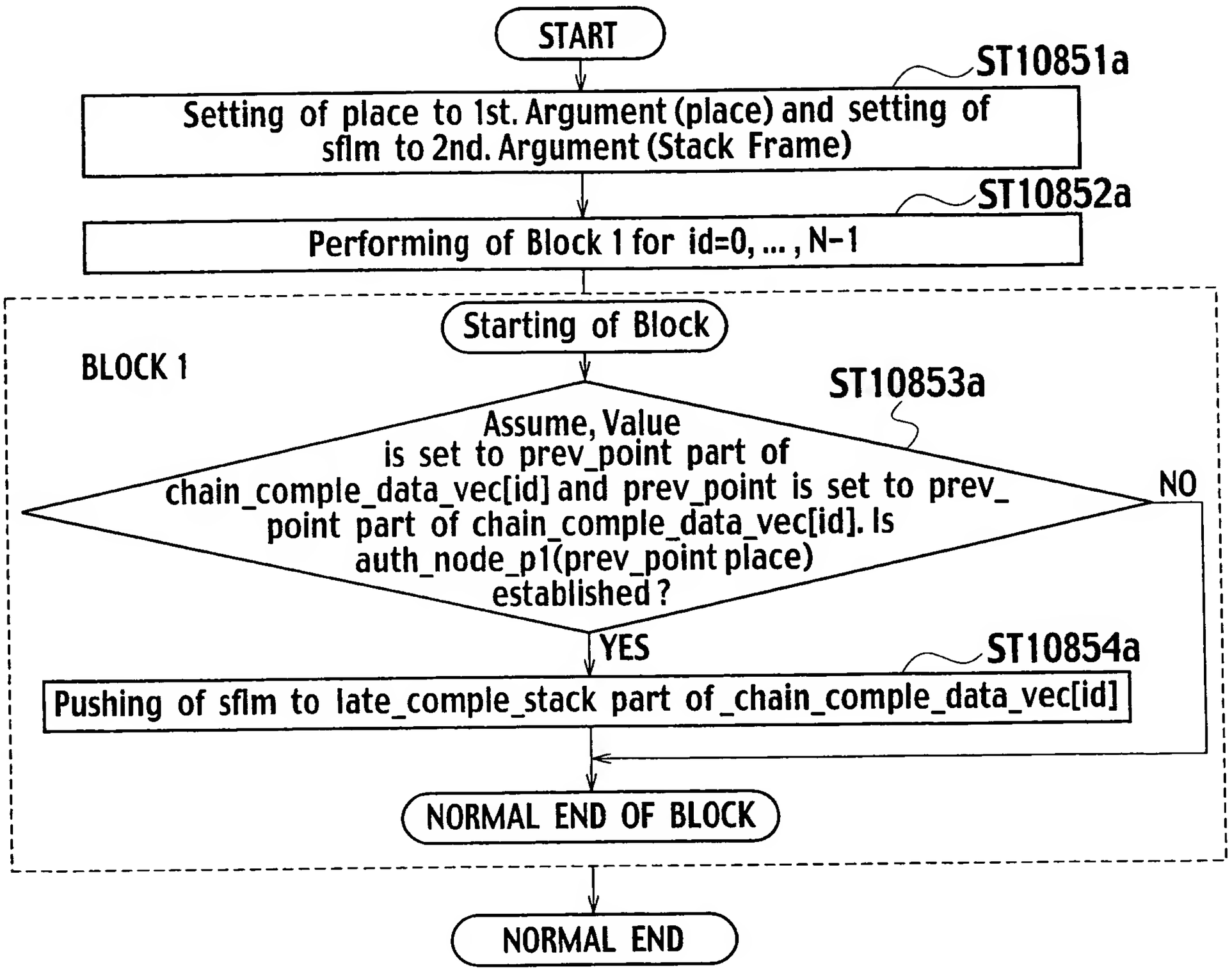

START
ST10851a
Setting of place to 1st. Argument (place) and setting of sflm to 2nd. Argument (Stack Frame)
ST10852a
Performing of Block 1 for id=0, ... , N-1
BLOCK 1
Starting of Block
ST10853a
Assume, Value is set to prev_point part of chain_comple_data_vec[id] and prev_point is set to prev_point part of chain_comple_data_vec[id]. Is auth_node_p1(prev_point place) established ?
NO
YES
ST10854a
Pushing of sflm to late_comple_stack part of _chain_comple_data_vec[id]
NORMAL END OF BLOCK
NORMAL END

FIG. 54

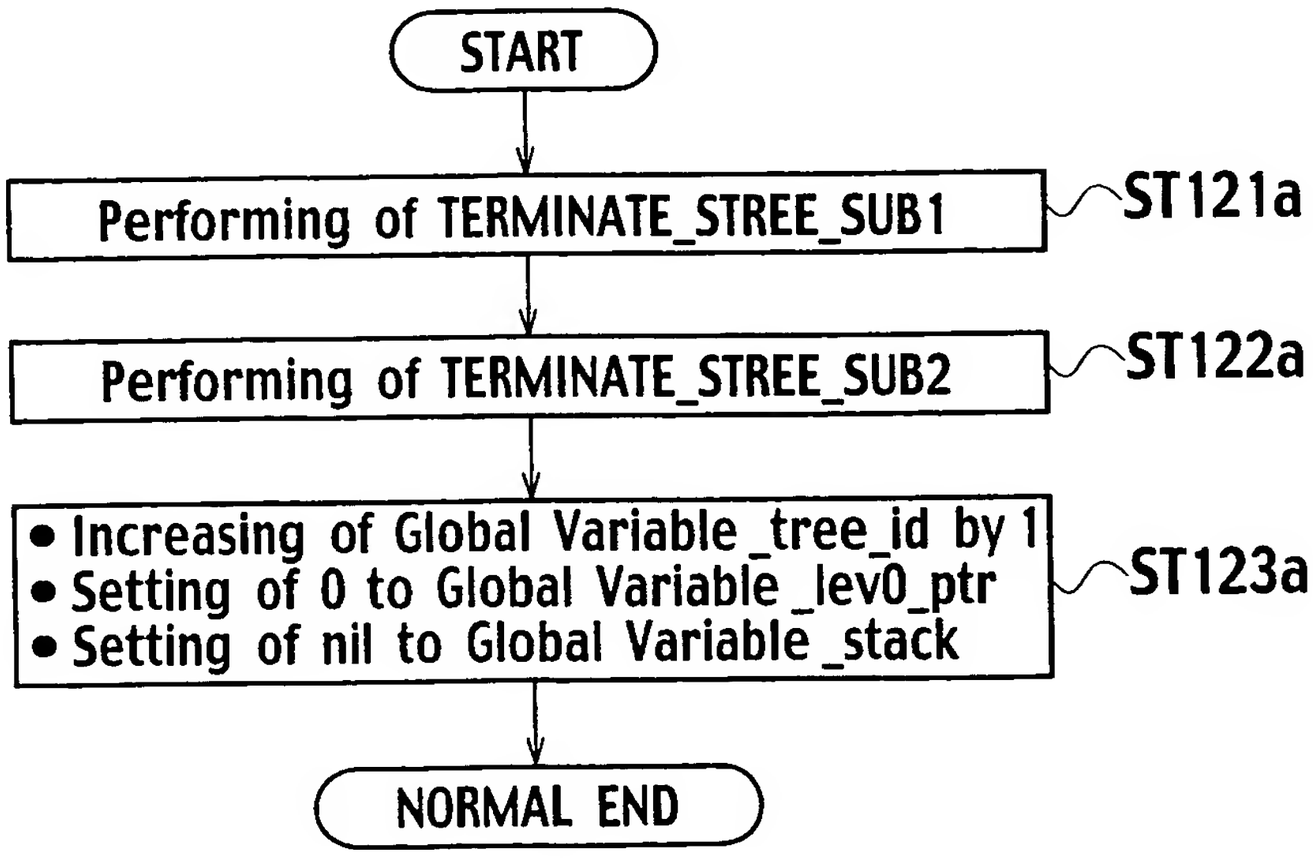

START
Performing of TERMINATE_STREE_SUB1
ST121a
Performing of TERMINATE_STREE_SUB2
ST122a
• Increasing of Global Variable _tree_id by 1
• Setting of 0 to Global Variable _lev0_ptr
• Setting of nil to Global Variable _stack
ST123a
NORMAL END

FIG. 55

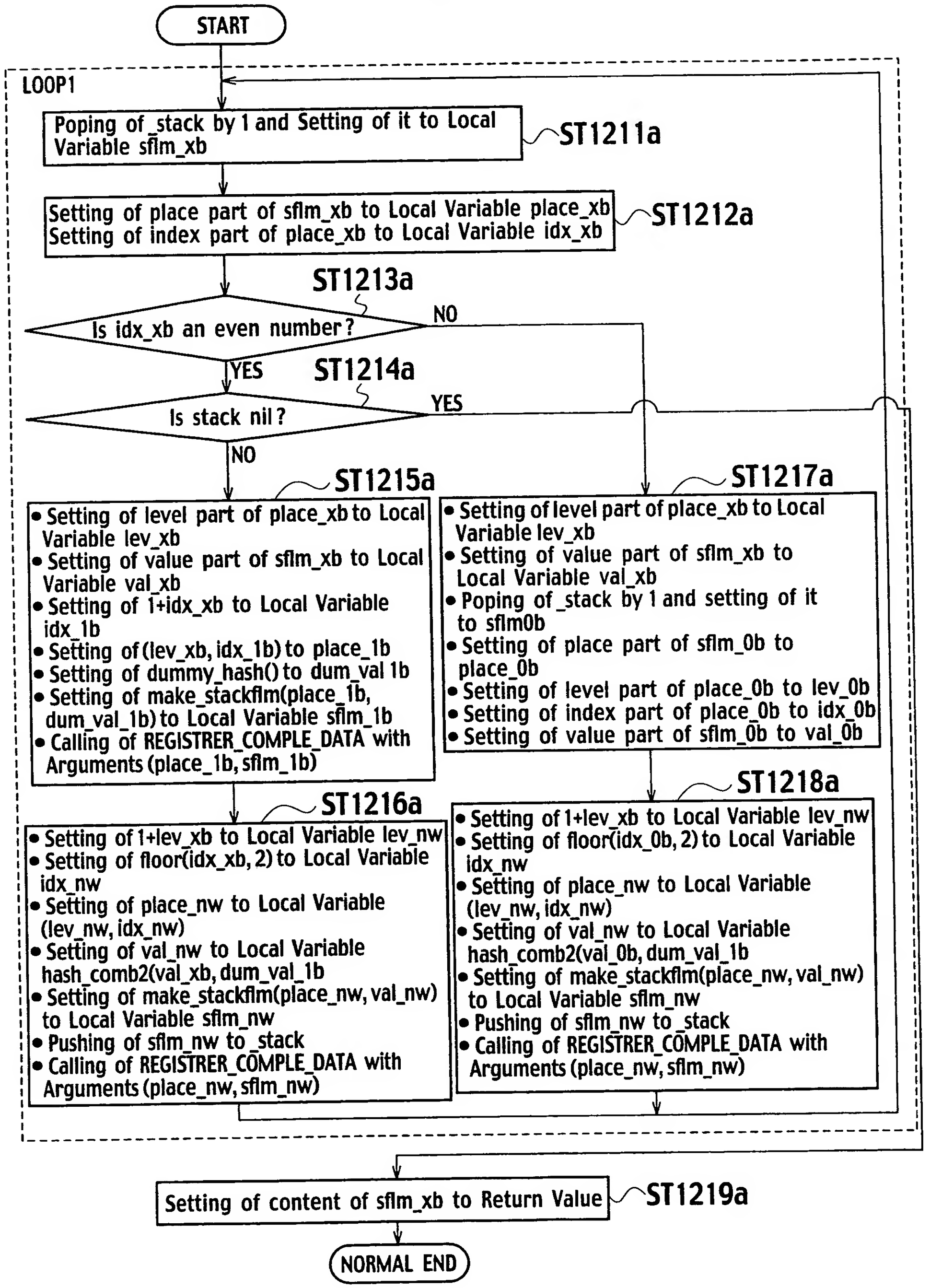

START
LOOP1
Poping of_stack by 1 and Setting of it to Local Variable sflm_xb
ST1211a
Setting of place part of sflm_xb to Local Variable place_xb
Setting of index part of place_xb to Local Variable idx_xb
ST1212a
ST1213a
Is idx_xb an even number?
NO
YES
ST1214a
Is stack nil?
YES
NO
ST1215a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sflm_xb to Local Variable val_xb
• Setting of 1+idx_xb to Local Variable idx_1b
• Setting of (lev_xb, idx_1b) to place_1b
• Setting of dummy_hash() to dum_val 1b
• Setting of make_stackflm(place_1b, dum_val_1b) to Local Variable sflm_1b
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_1b, sflm_1b)
ST1216a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_xb, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_xb, dum_val_1b
• Setting of make_stackflm(place_nw, val_nw) to Local Variable sflm_nw
• Pushing of sflm_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sflm_nw)
ST1217a
• Setting of level part of place_xb to Local Variable lev_xb
• Setting of value part of sflm_xb to Local Variable val_xb
• Poping of_stack by 1 and setting of it to sflm0b
• Setting of place part of sflm_0b to place_0b
• Setting of level part of place_0b to lev_0b
• Setting of index part of place_0b to idx_0b
• Setting of value part of sflm_0b to val_0b
ST1218a
• Setting of 1+lev_xb to Local Variable lev_nw
• Setting of floor(idx_0b, 2) to Local Variable idx_nw
• Setting of place_nw to Local Variable (lev_nw, idx_nw)
• Setting of val_nw to Local Variable hash_comb2(val_0b, dum_val_1b
• Setting of make_stackflm(place_nw, val_nw) to Local Variable sflm_nw
• Pushing of sflm_nw to _stack
• Calling of REGISTRER_COMPLE_DATA with Arguments (place_nw, sflm_nw)
Setting of content of sflm_xb to Return Value
ST1219a
NORMAL END

FIG. 56

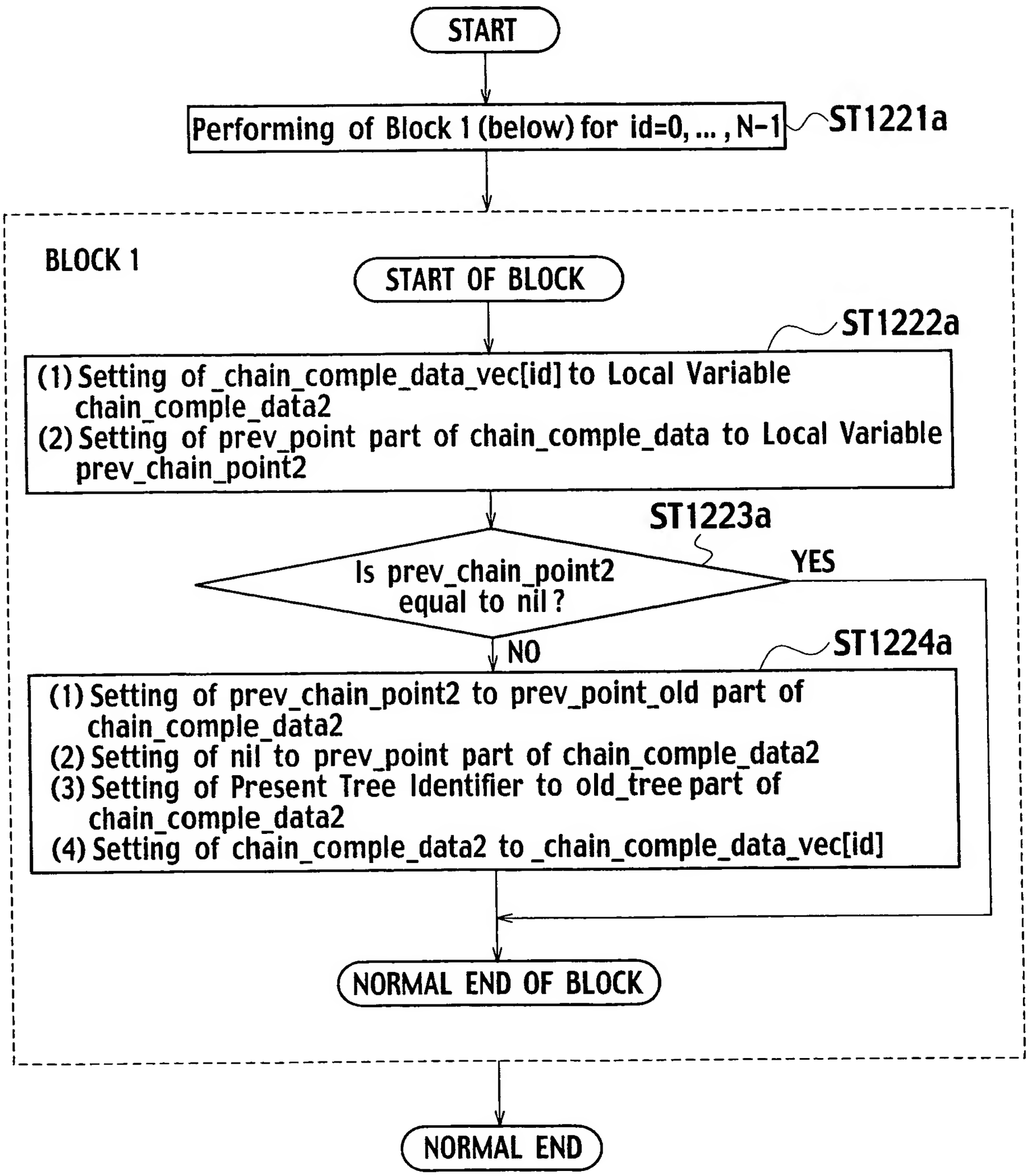
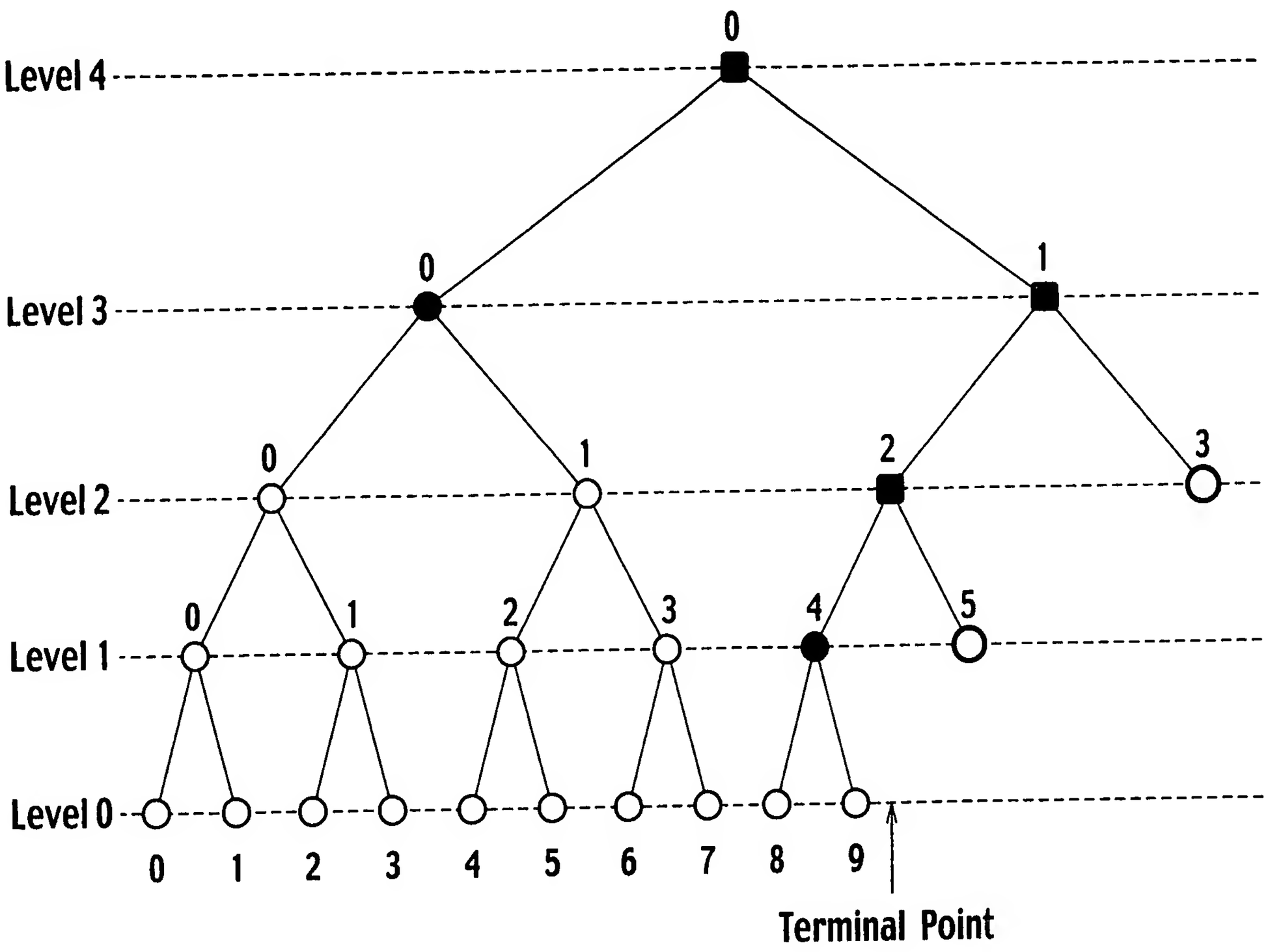
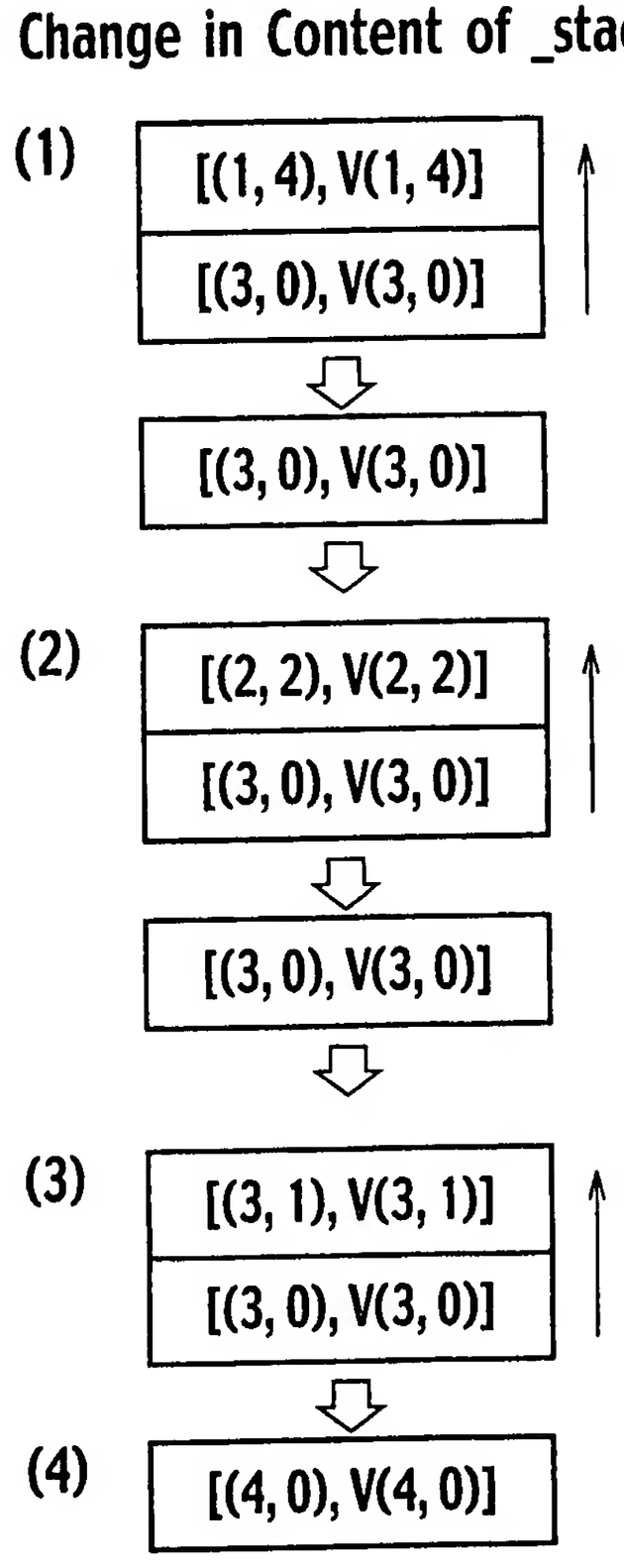

START
Performing of Block 1 (below) for id=0, ... , N-1
ST1221a
BLOCK 1
START OF BLOCK
ST1222a
(1) Setting of _chain_comple_data_vec[id] to Local Variable chain_comple_data2
(2) Setting of prev_point part of chain_comple_data to Local Variable prev_chain_point2
ST1223a
Is prev_chain_point2 equal to nil ?
YES
NO
ST1224a
(1) Setting of prev_chain_point2 to prev_point_old part of chain_comple_data2
(2) Setting of nil to prev_point part of chain_comple_data2
(3) Setting of Present Tree Identifier to old_tree part of chain_comple_data2
(4) Setting of chain_comple_data2 to _chain_comple_data_vec[id]
NORMAL END OF BLOCK
NORMAL END

FIG. 57





Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 51 of 77

FIG. 58

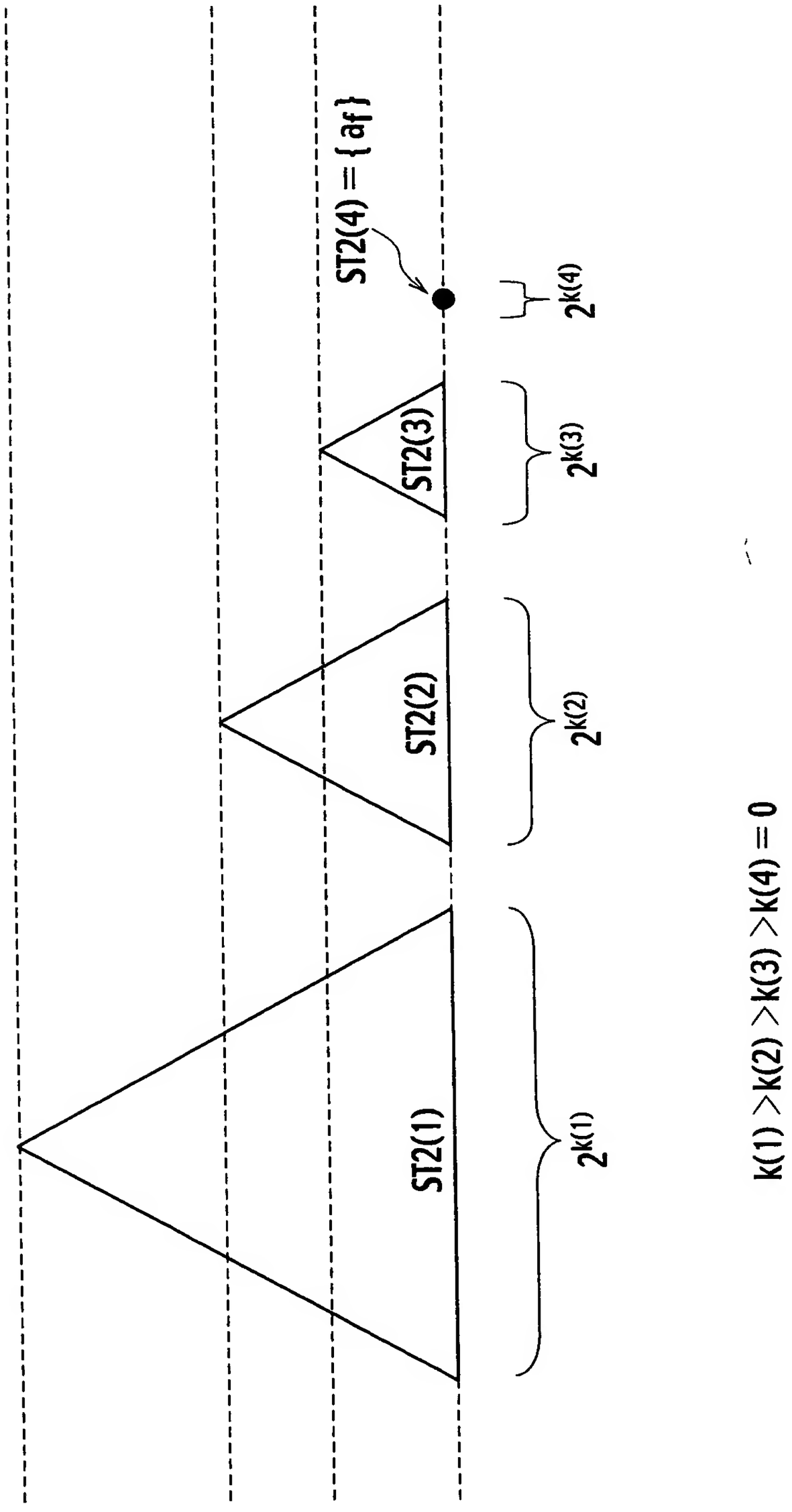
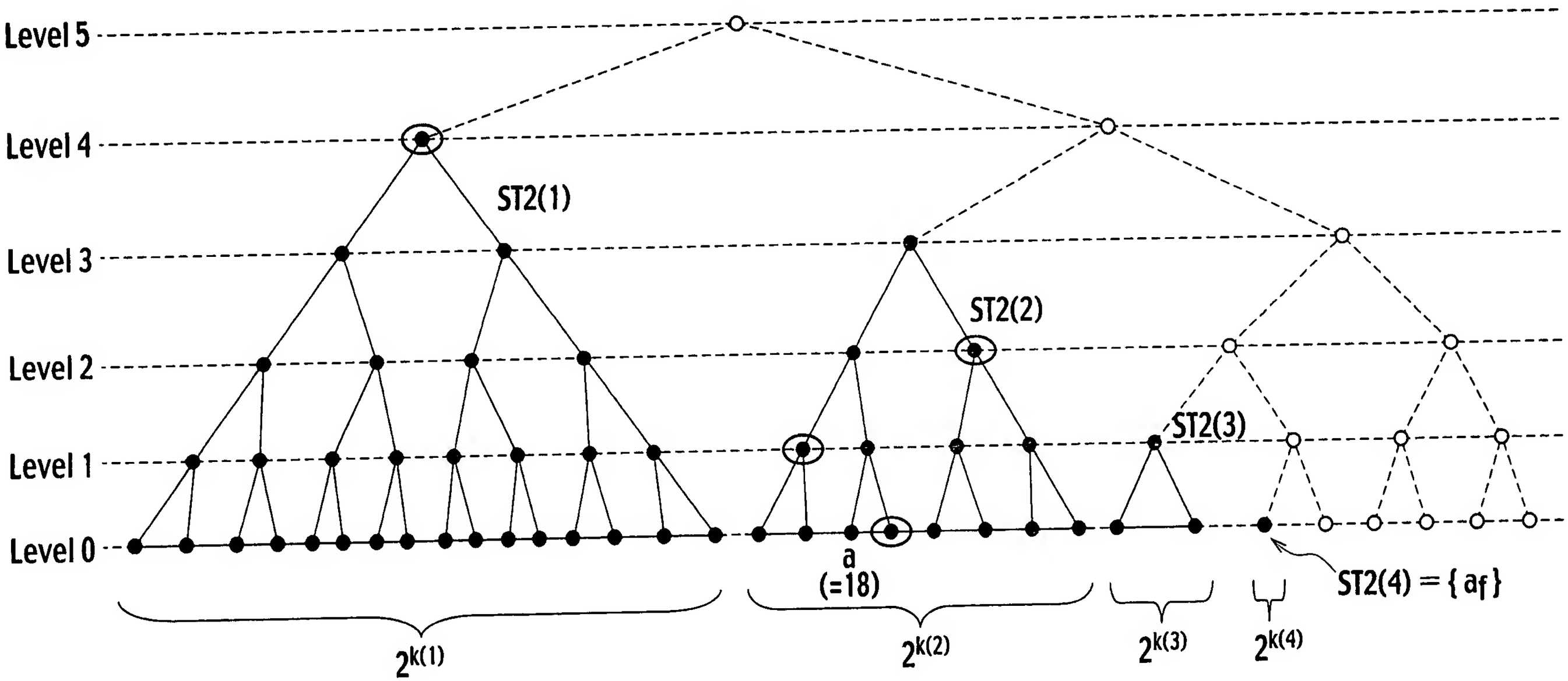


FIG. 59



k(1)=4 >k(2)=3 >k(3)=1 >k(4) = 0

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 53 of 77

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 54 of 77

FIG. 60

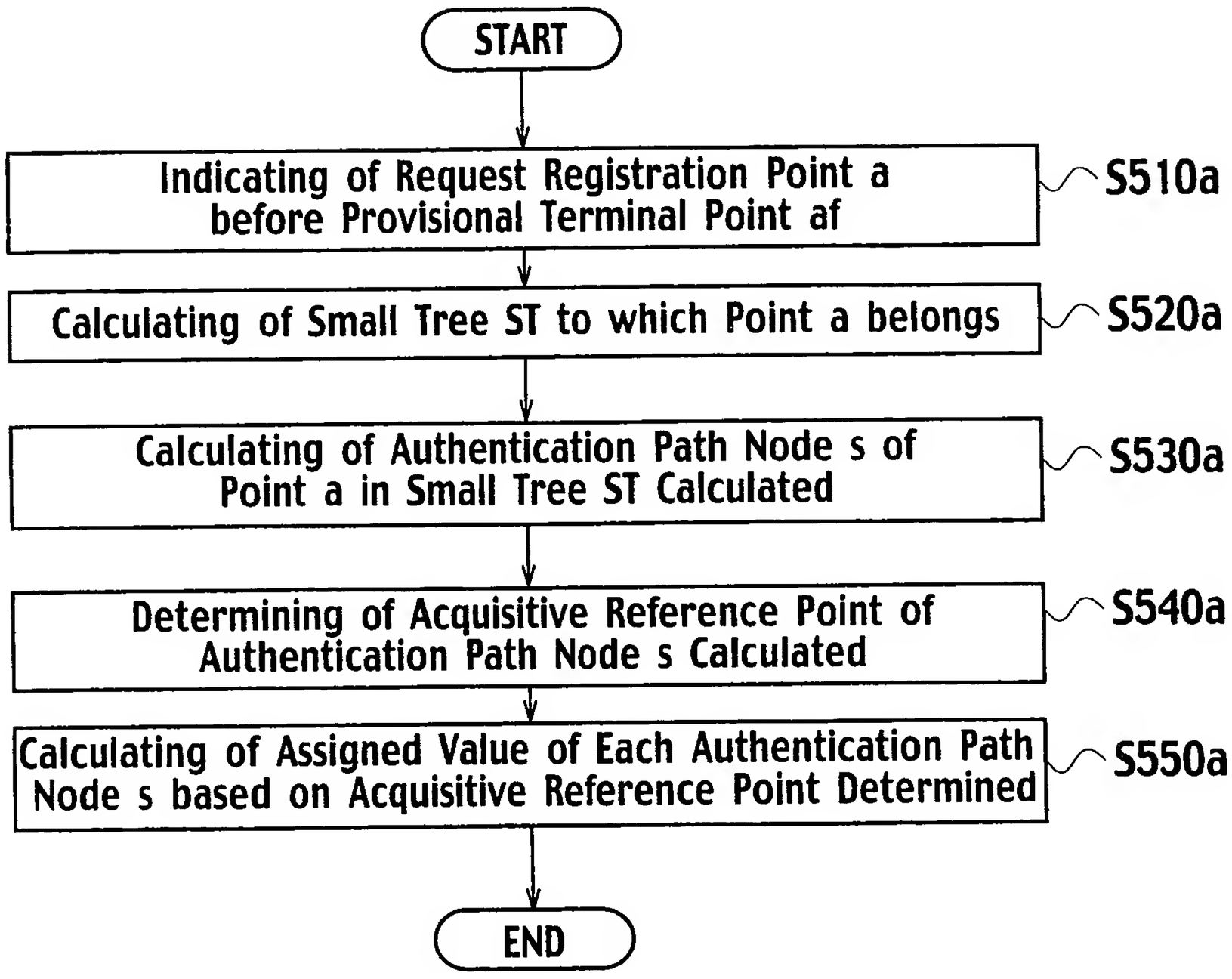
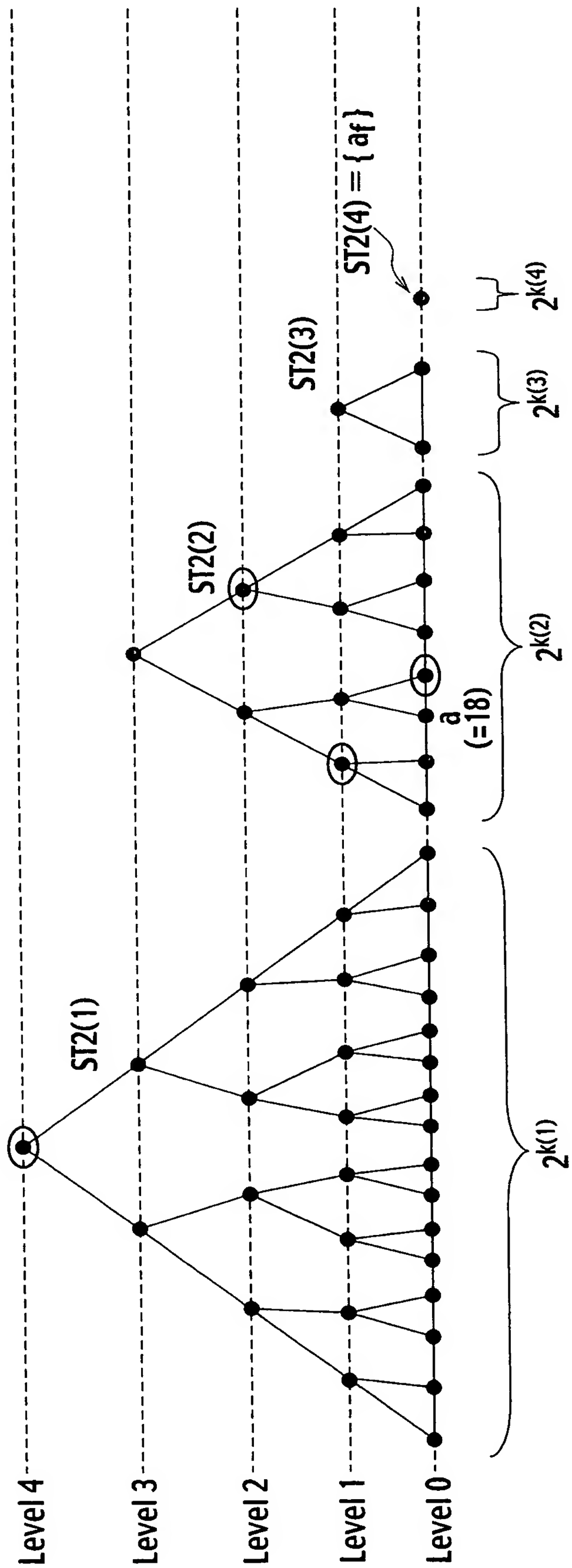


FIG. 61


Level 4
Level 3
Level 2
Level 1
Level 0
ST2(1)
ST2(2)
ST2(3)
ST2(4) = {af}
a
(=18)
$2^{k(1)}$
$2^{k(2)}$
$2^{k(3)}$
$2^{k(4)}$
K(1)=4 >K(2)=3 >K(3)=1 >K(4)=0

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 56 of 77

FIG. 62

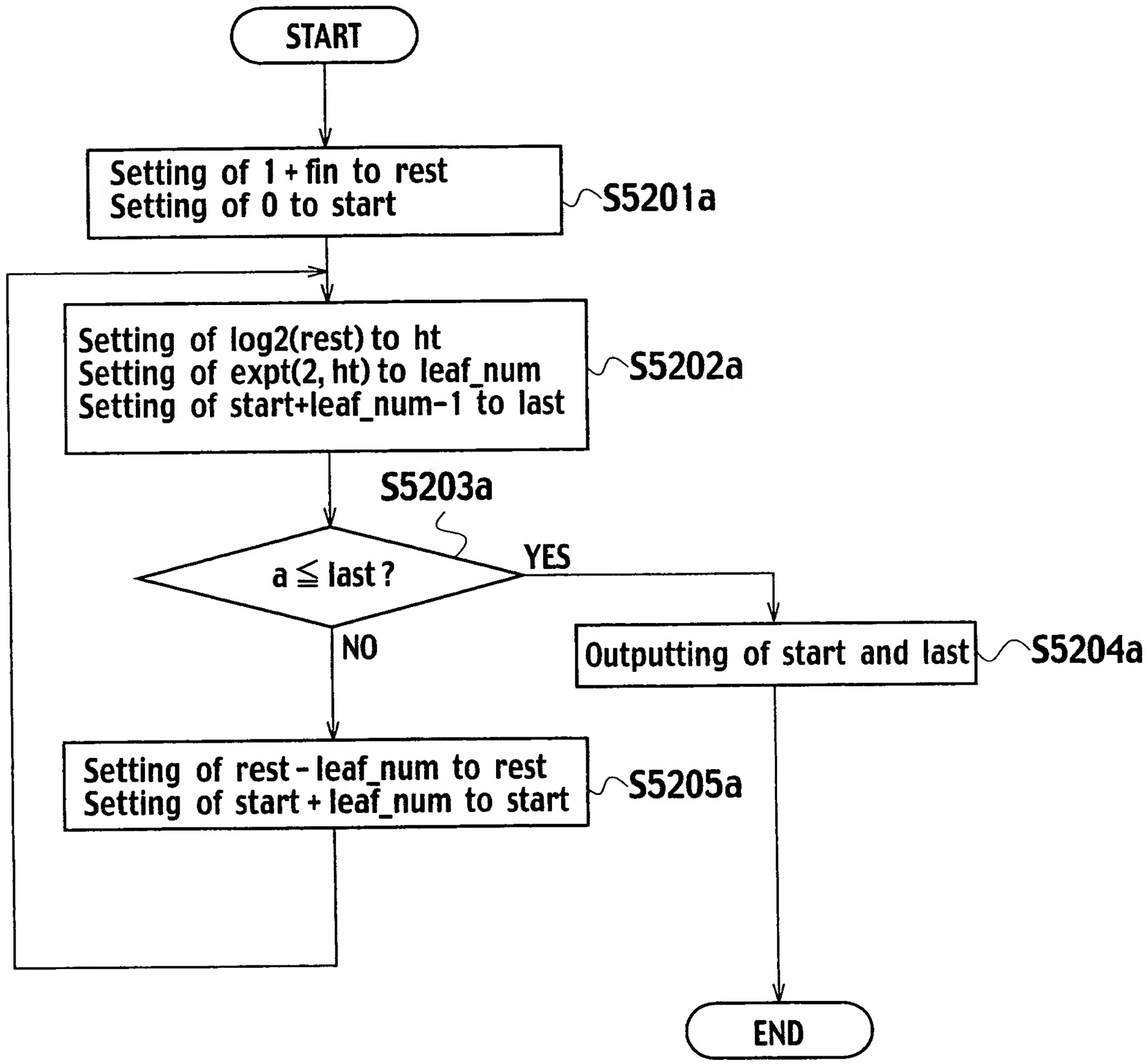


FIG. 63

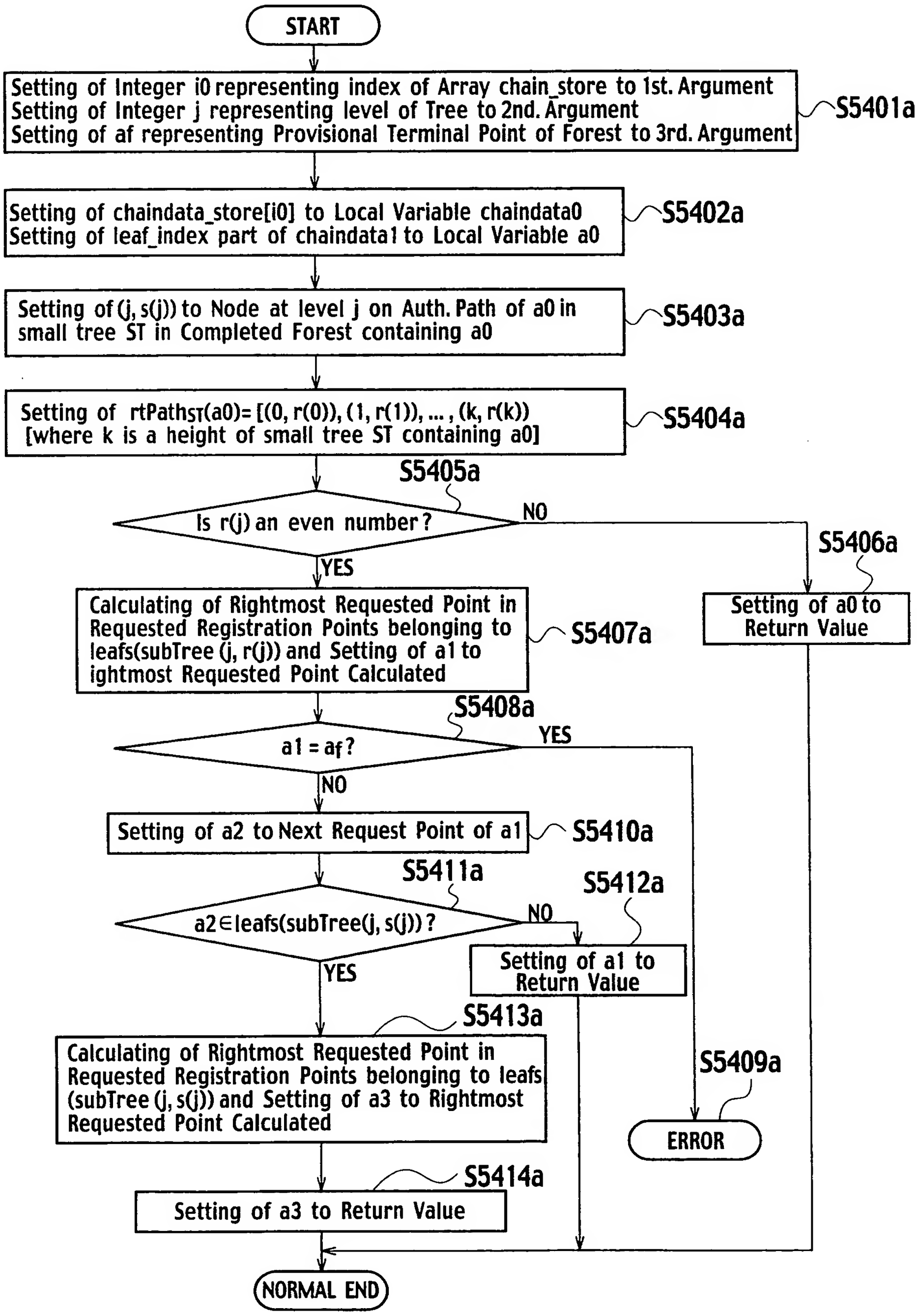
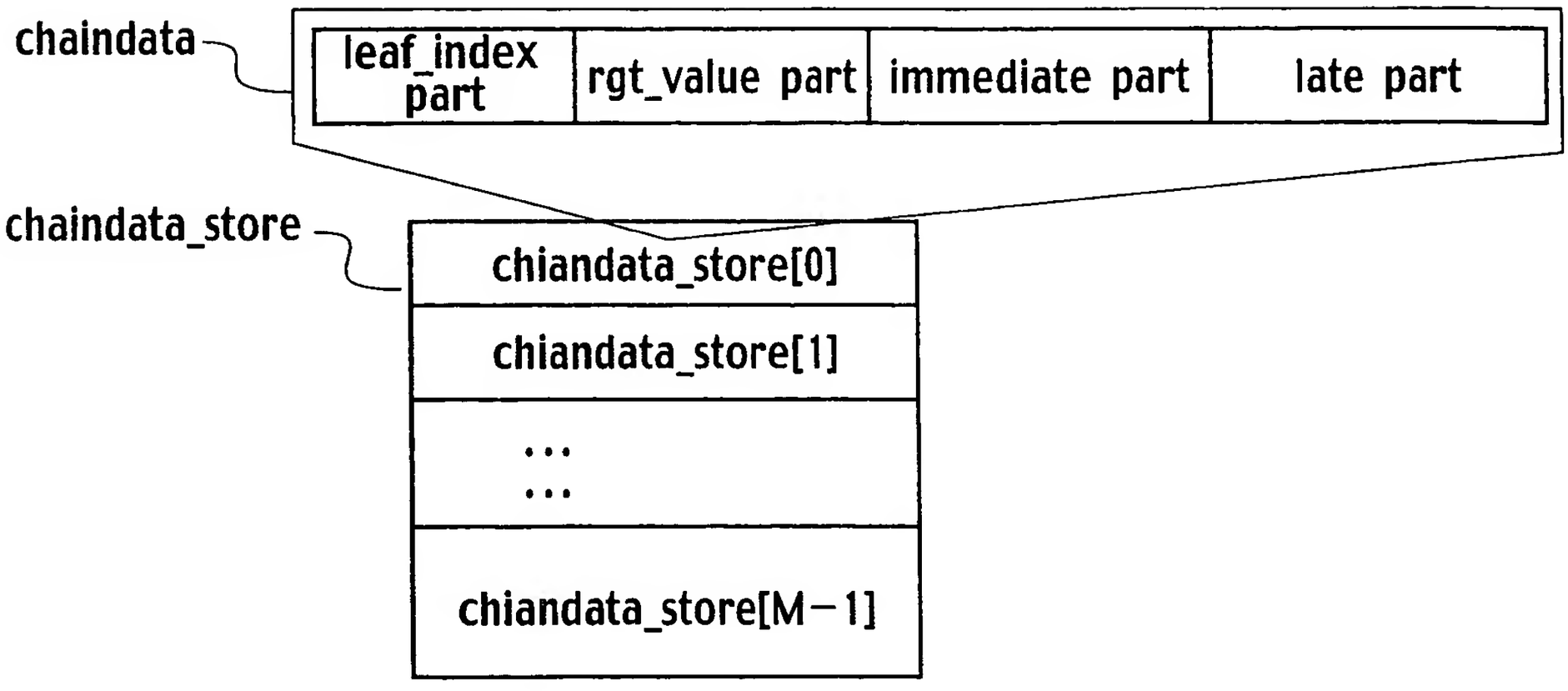

START
Setting of Integer i0 representing index of Array chain_store to 1st. Argument
Setting of Integer j representing level of Tree to 2nd. Argument
Setting of af representing Provisional Terminal Point of Forest to 3rd. Argument
S5401a
Setting of chaindata_store[i0] to Local Variable chaindata0
Setting of leaf_index part of chaindata1 to Local Variable a0
S5402a
Setting of (j, s(j)) to Node at level j on Auth. Path of a0 in small tree ST in Completed Forest containing a0
S5403a
Setting of rtPathsT(a0)= [(0, r(0)), (1, r(1)), ... , (k, r(k))
[where k is a height of small tree ST containing a0]
S5404a
S5405a
Is r(j) an even number?
NO
YES
S5406a
Setting of a0 to Return Value
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs(subTree (j, r(j)) and Setting of a1 to ightmost Requested Point Calculated
S5407a
S5408a
a1 = af?
YES
NO
Setting of a2 to Next Request Point of a1
S5410a
S5411a
a2∈leafs(subTree(j, s(j))?
NO
S5412a
Setting of a1 to Return Value
YES
S5413a
Calculating of Rightmost Requested Point in Requested Registration Points belonging to leafs (subTree (j, s(j)) and Setting of a3 to Rightmost Requested Point Calculated
S5409a
ERROR
S5414a
Setting of a3 to Return Value
NORMAL END

FIG. 64


chaindata
leaf_index part
rgt_value part
immediate part
late part
chaindata_store
chiandata_store[0]
chiandata_store[1]
...
chiandata_store[M−1]

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 59 of 77

FIG. 65A

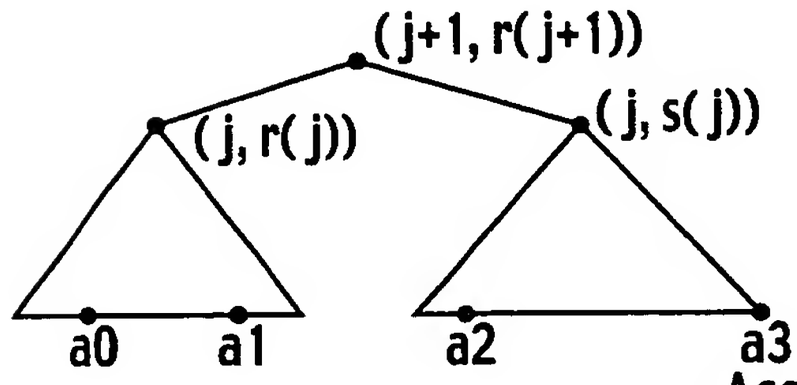


FIG. 65B

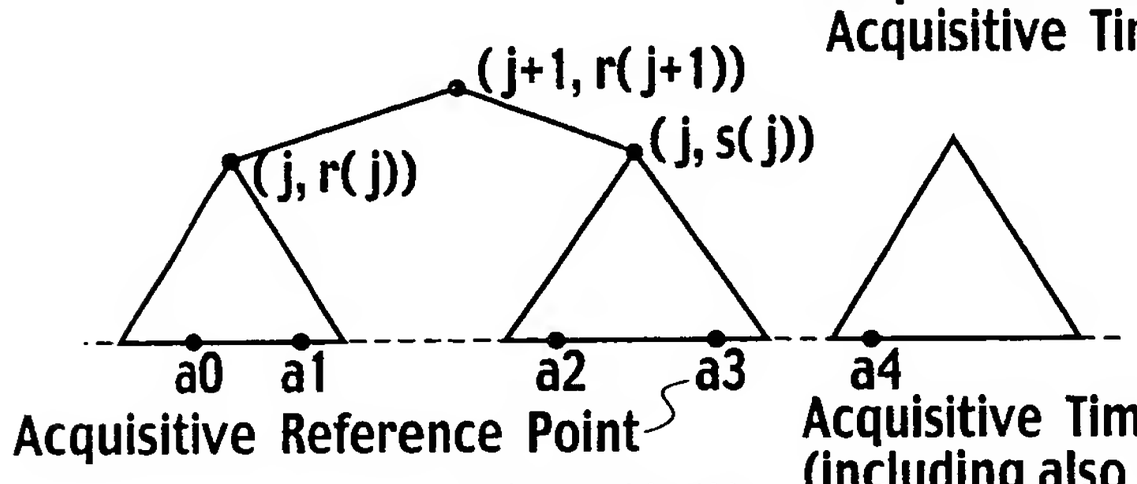


FIG. 65C

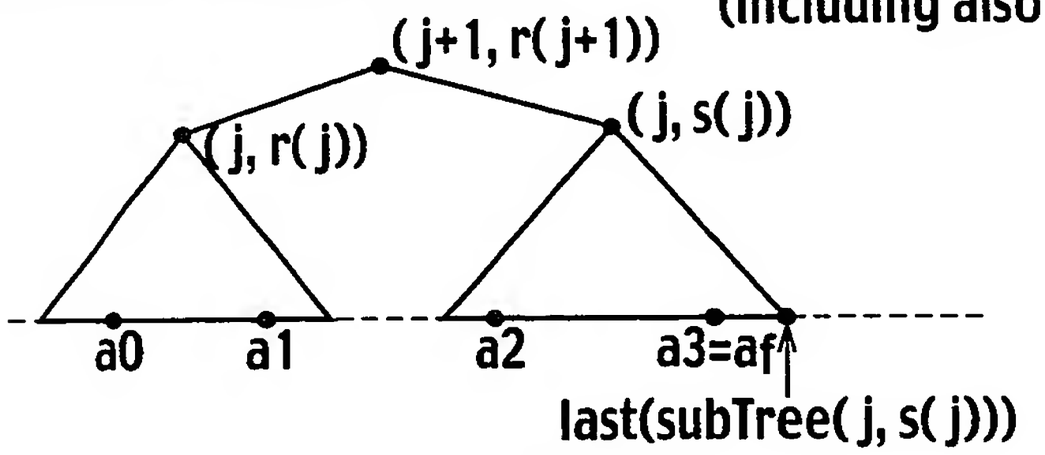


FIG. 65D

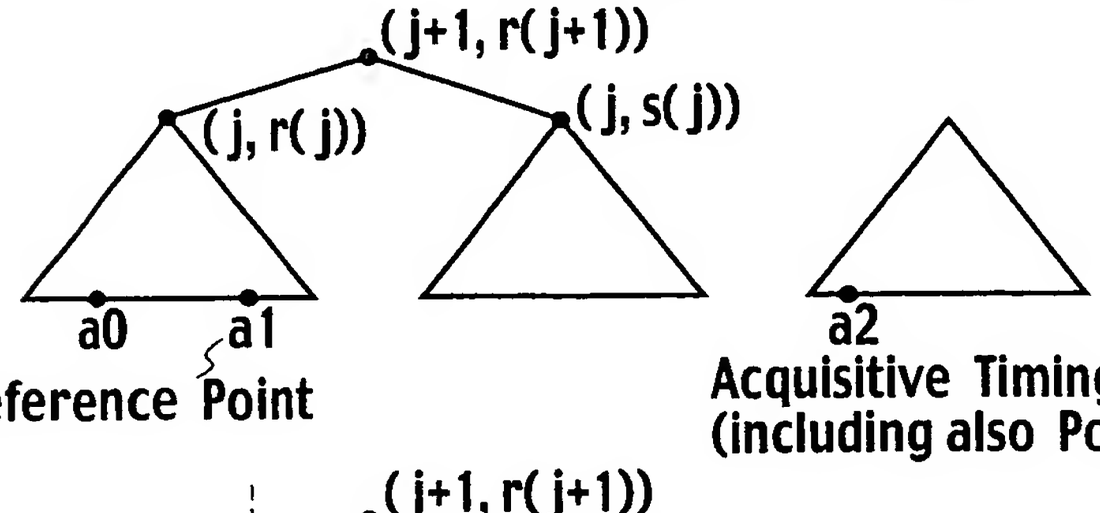


FIG. 65E

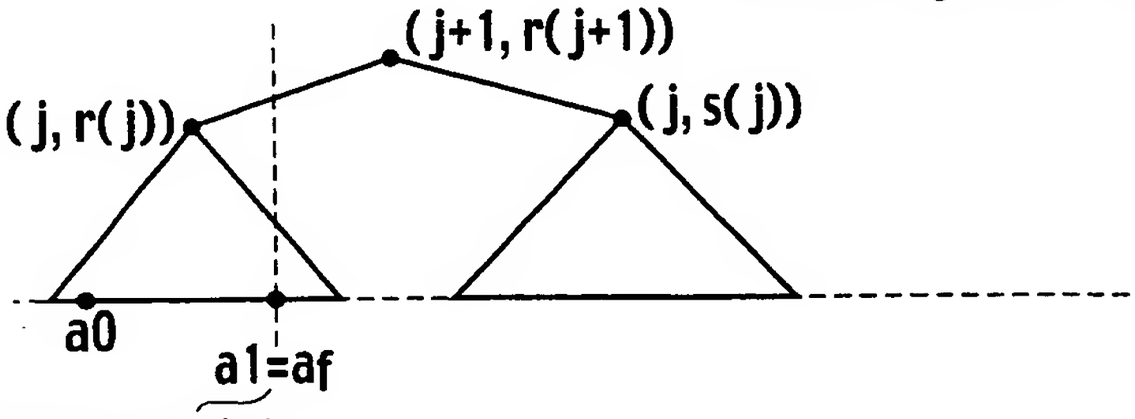


FIG. 65F

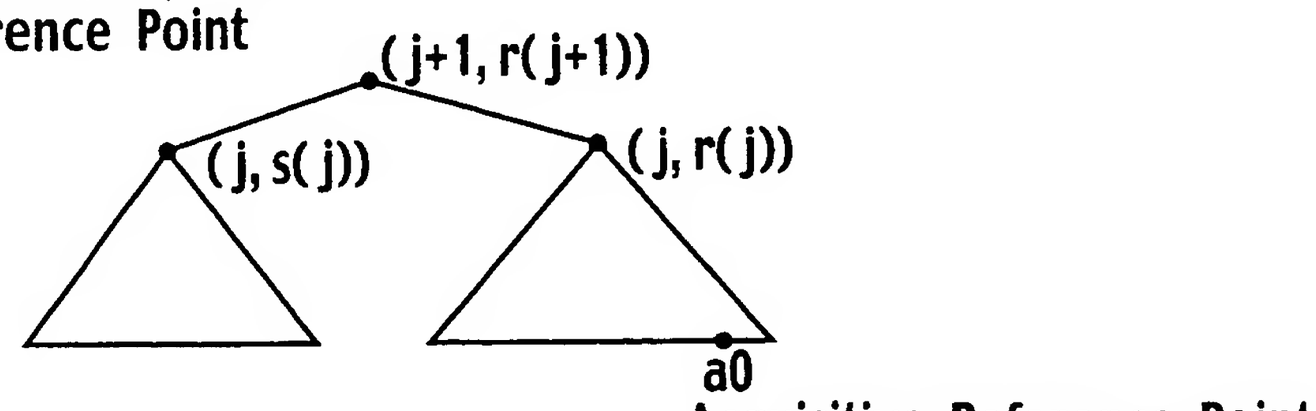


FIG. 66

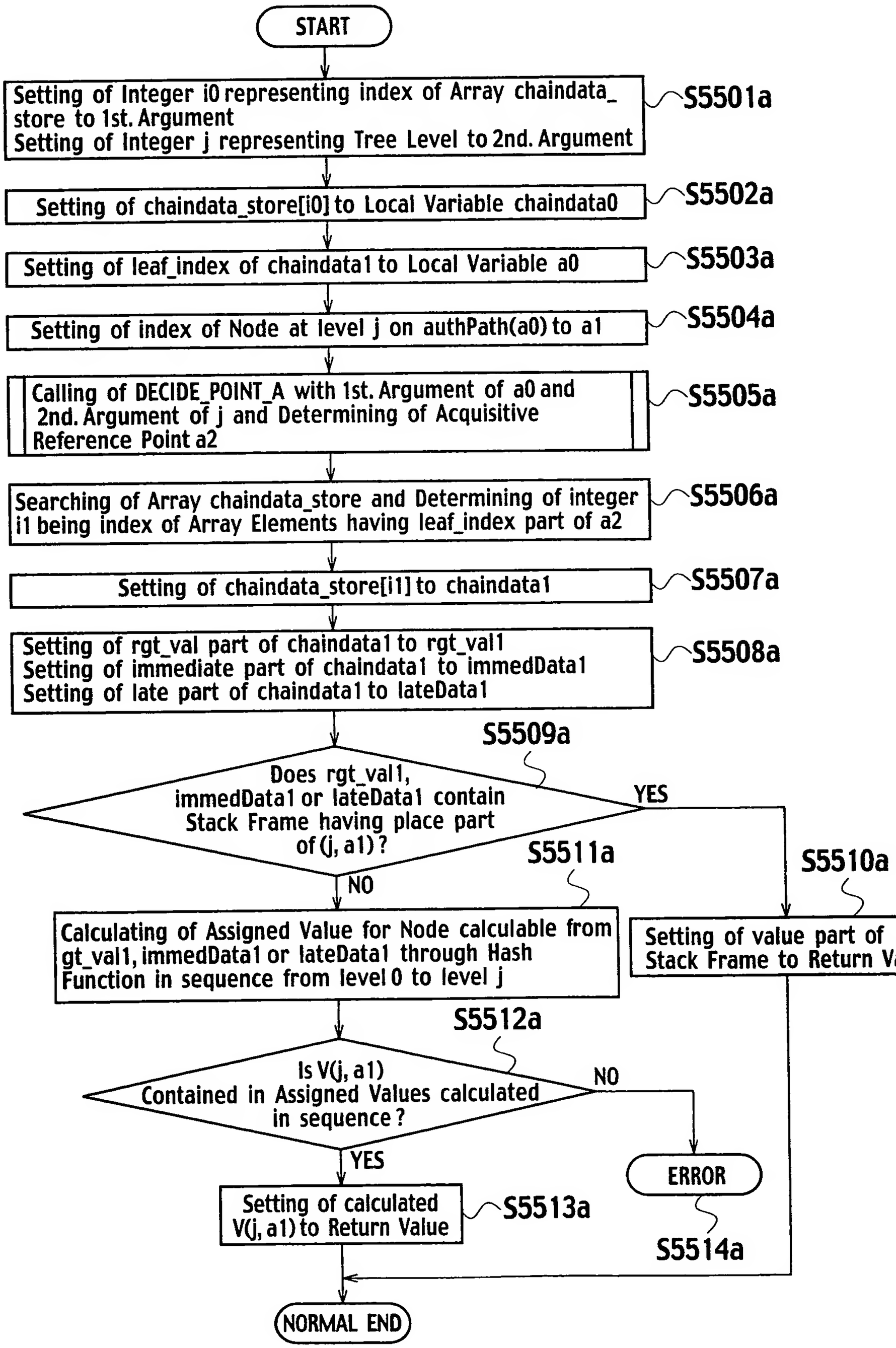

START
Setting of Integer i0 representing index of Array chaindata_store to 1st. Argument
Setting of Integer j representing Tree Level to 2nd. Argument
S5501a
Setting of chaindata_store[i0] to Local Variable chaindata0
S5502a
Setting of leaf_index of chaindata1 to Local Variable a0
S5503a
Setting of index of Node at level j on authPath(a0) to a1
S5504a
Calling of DECIDE_POINT_A with 1st. Argument of a0 and 2nd. Argument of j and Determining of Acquisitive Reference Point a2
S5505a
Searching of Array chaindata_store and Determining of integer i1 being index of Array Elements having leaf_index part of a2
S5506a
Setting of chaindata_store[i1] to chaindata1
S5507a
Setting of rgt_val part of chaindata1 to rgt_val1
Setting of immediate part of chaindata1 to immedData1
Setting of late part of chaindata1 to lateData1
S5508a
S5509a
Does rgt_val1, immedData1 or lateData1 contain Stack Frame having place part of (j, a1)?
YES
NO
S5510a
S5511a
Calculating of Assigned Value for Node calculable from gt_val1, immedData1 or lateData1 through Hash Function in sequence from level 0 to level j
Setting of value part of Stack Frame to Return Value
S5512a
Is V(j, a1) Contained in Assigned Values calculated in sequence?
NO
YES
ERROR
Setting of calculated V(j, a1) to Return Value
S5513a
S5514a
NORMAL END

FIG. 67

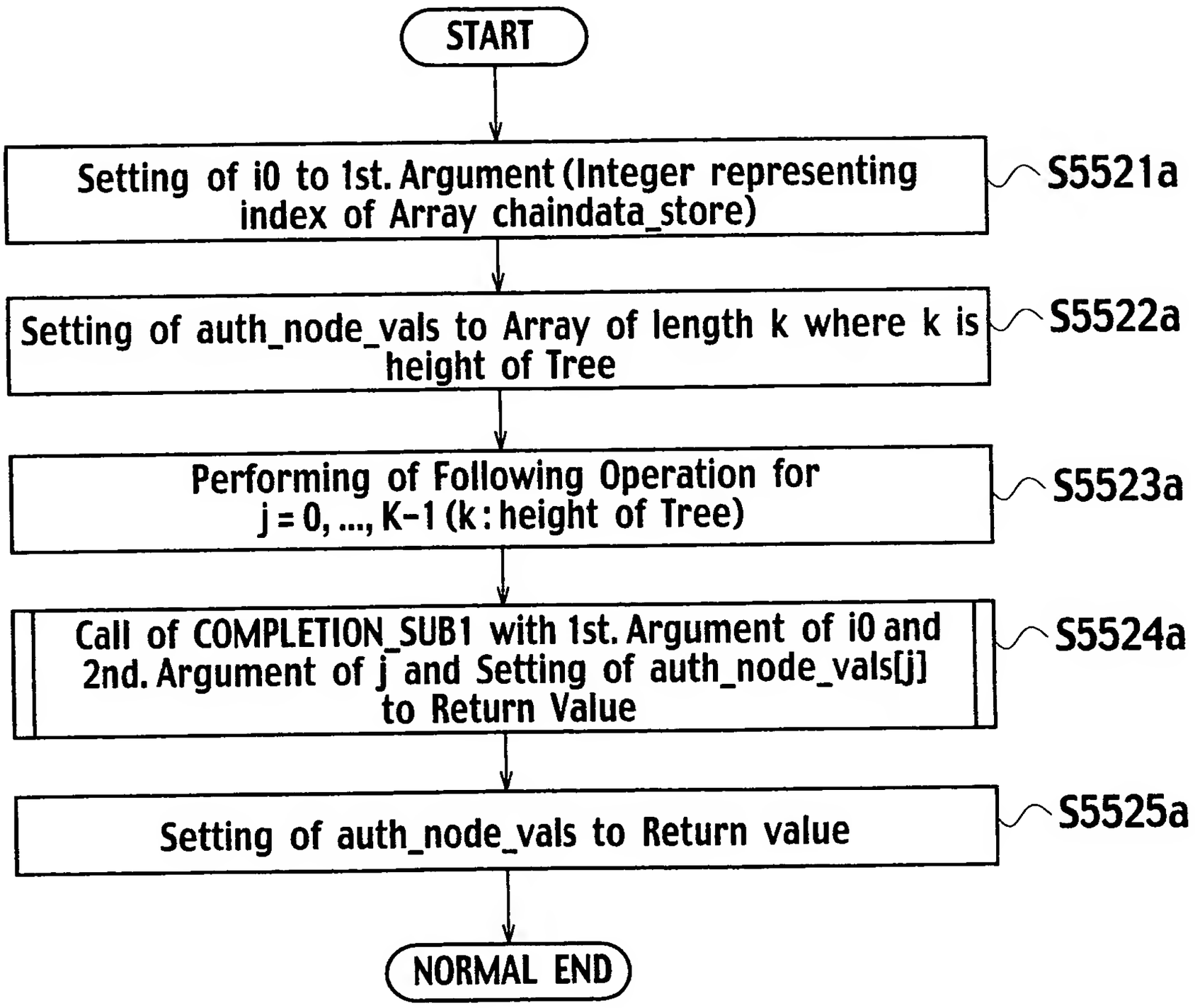

START
Setting of i0 to 1st. Argument (Integer representing index of Array chaindata_store)
S5521a
Setting of auth_node_vals to Array of length k where k is height of Tree
S5522a
Performing of Following Operation for j = 0, ..., K-1 (k : height of Tree)
S5523a
Call of COMPLETION_SUB1 with 1st. Argument of i0 and 2nd. Argument of j and Setting of auth_node_vals[j] to Return Value
S5524a
Setting of auth_node_vals to Return value
S5525a
NORMAL END

FIG. 68

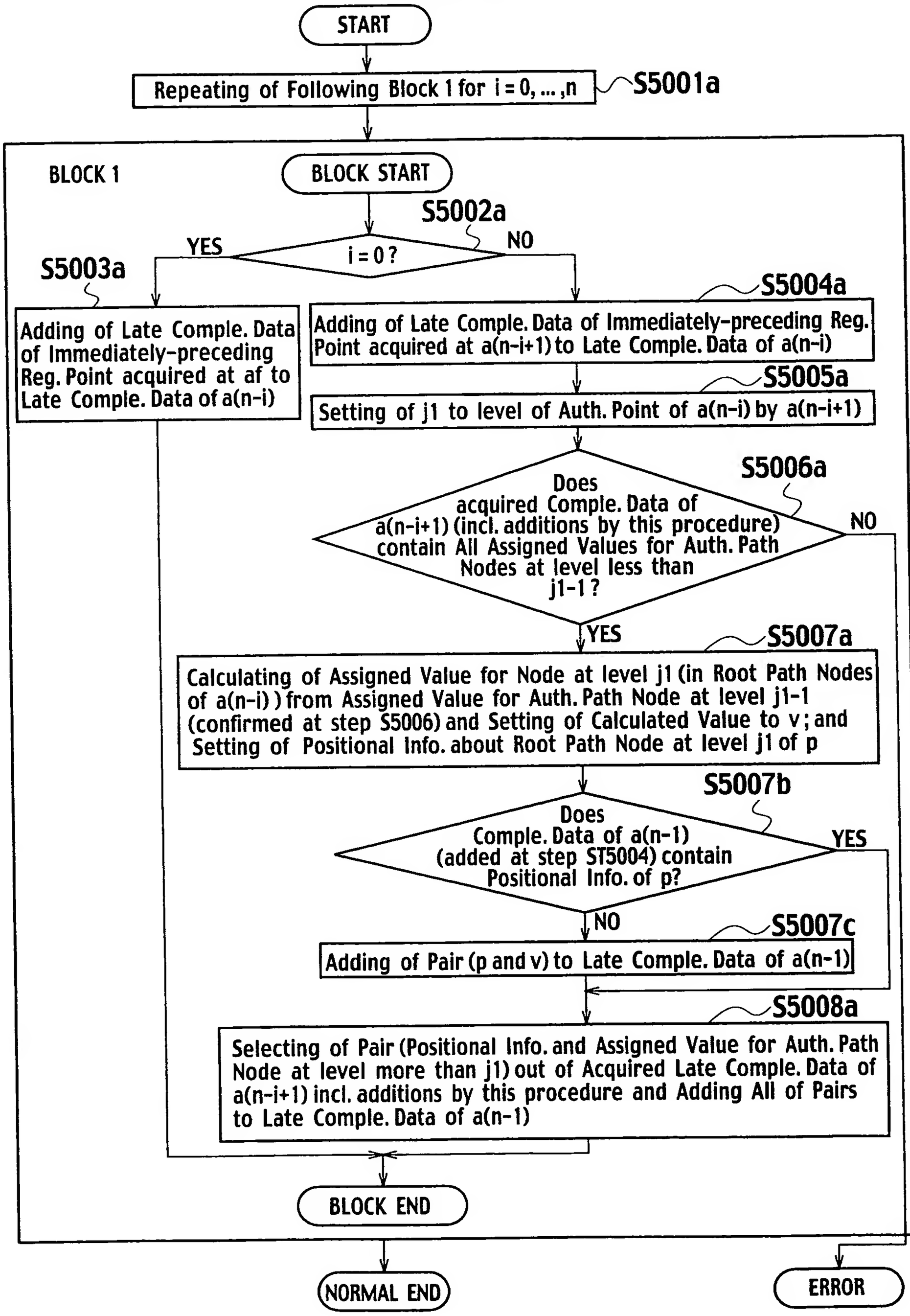
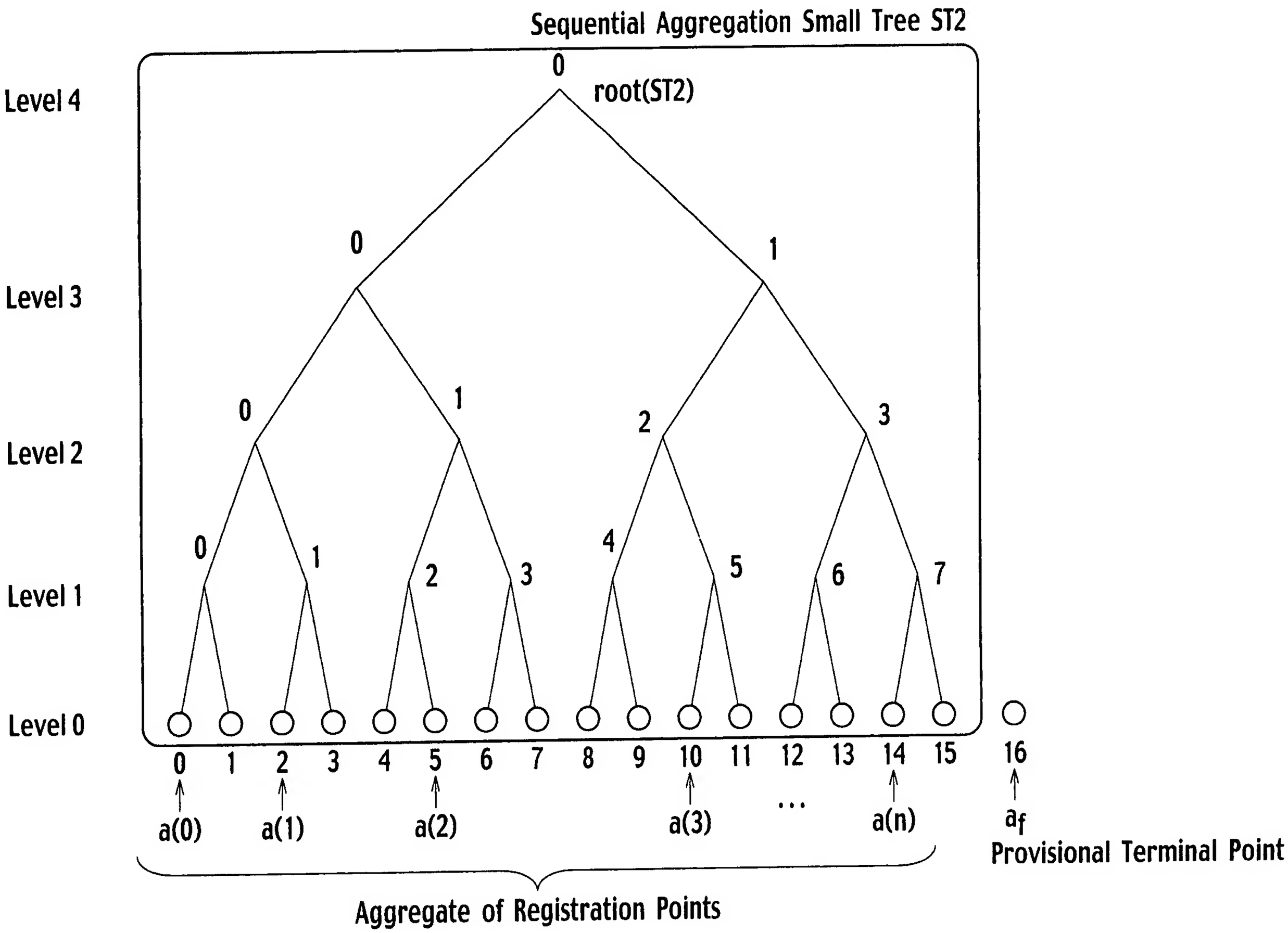
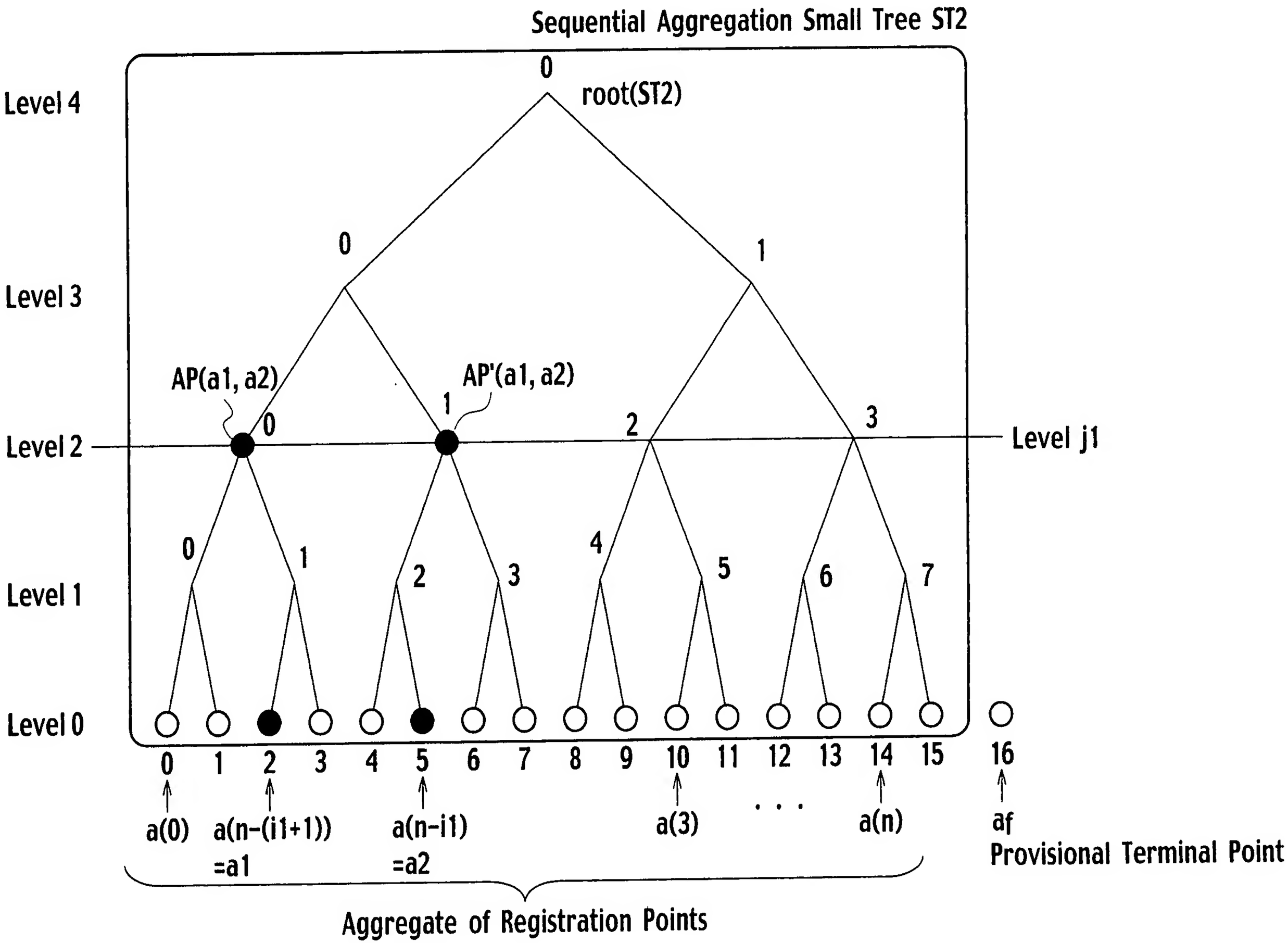

START
Repeating of Following Block 1 for i = 0, ... ,n
S5001a
BLOCK 1
BLOCK START
S5002a
i = 0 ?
YES
NO
S5003a
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at af to Late Comple. Data of a(n-i)
S5004a
Adding of Late Comple. Data of Immediately-preceding Reg. Point acquired at a(n-i+1) to Late Comple. Data of a(n-i)
S5005a
Setting of j1 to level of Auth. Point of a(n-i) by a(n-i+1)
S5006a
Does acquired Comple. Data of a(n-i+1) (incl. additions by this procedure) contain All Assigned Values for Auth. Path Nodes at level less than j1-1 ?
NO
YES
S5007a
Calculating of Assigned Value for Node at level j1 (in Root Path Nodes of a(n-i)) from Assigned Value for Auth. Path Node at level j1-1 (confirmed at step S5006) and Setting of Calculated Value to v; and Setting of Positional Info. about Root Path Node at level j1 of p
S5007b
Does Comple. Data of a(n-1) (added at step ST5004) contain Positional Info. of p?
YES
NO
S5007c
Adding of Pair (p and v) to Late Comple. Data of a(n-1)
S5008a
Selecting of Pair (Positional Info. and Assigned Value for Auth. Path Node at level more than j1) out of Acquired Late Comple. Data of a(n-i+1) incl. additions by this procedure and Adding All of Pairs to Late Comple. Data of a(n-1)
BLOCK END
NORMAL END
ERROR

FIG. 69



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500

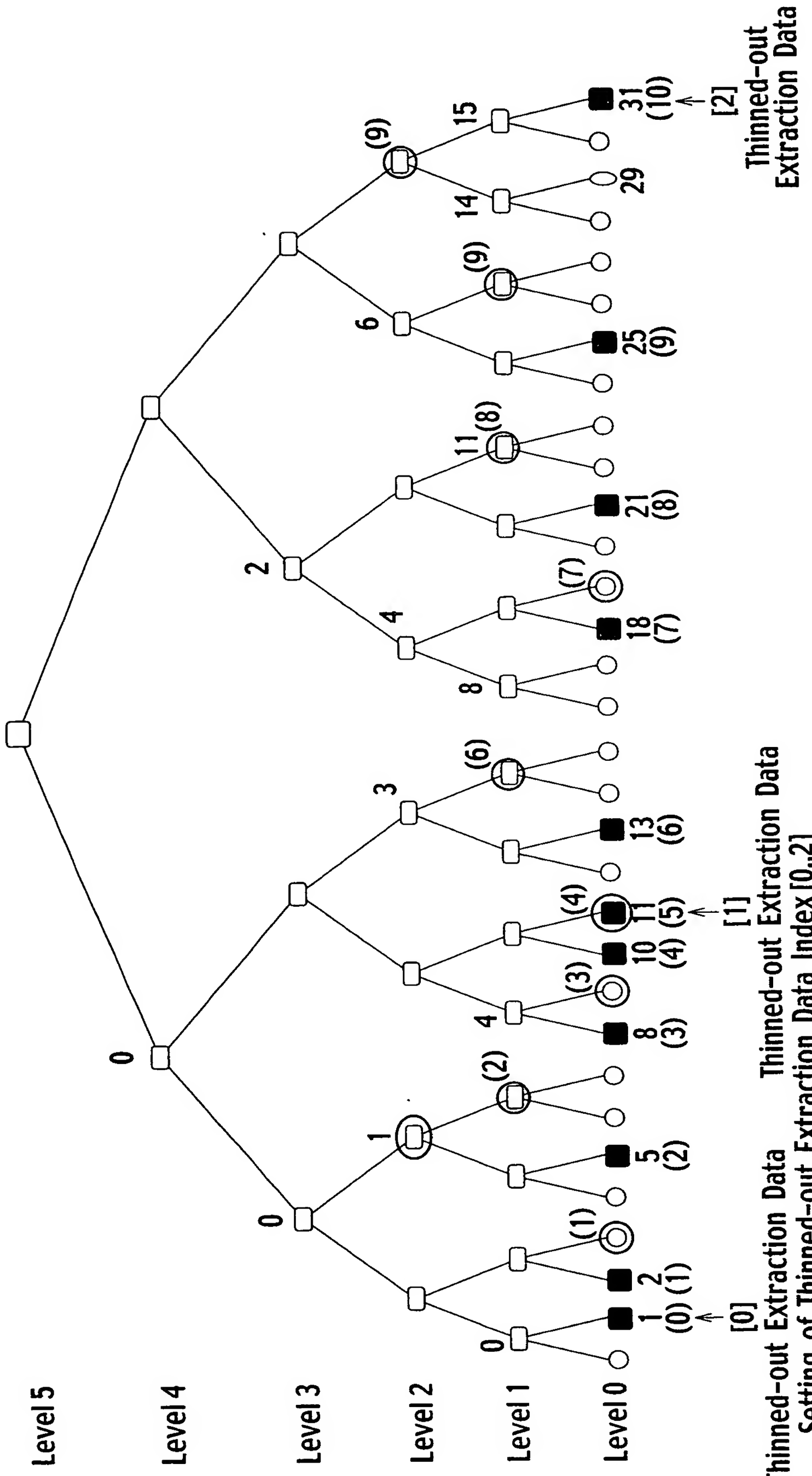
FIG. 70



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 64 of 77

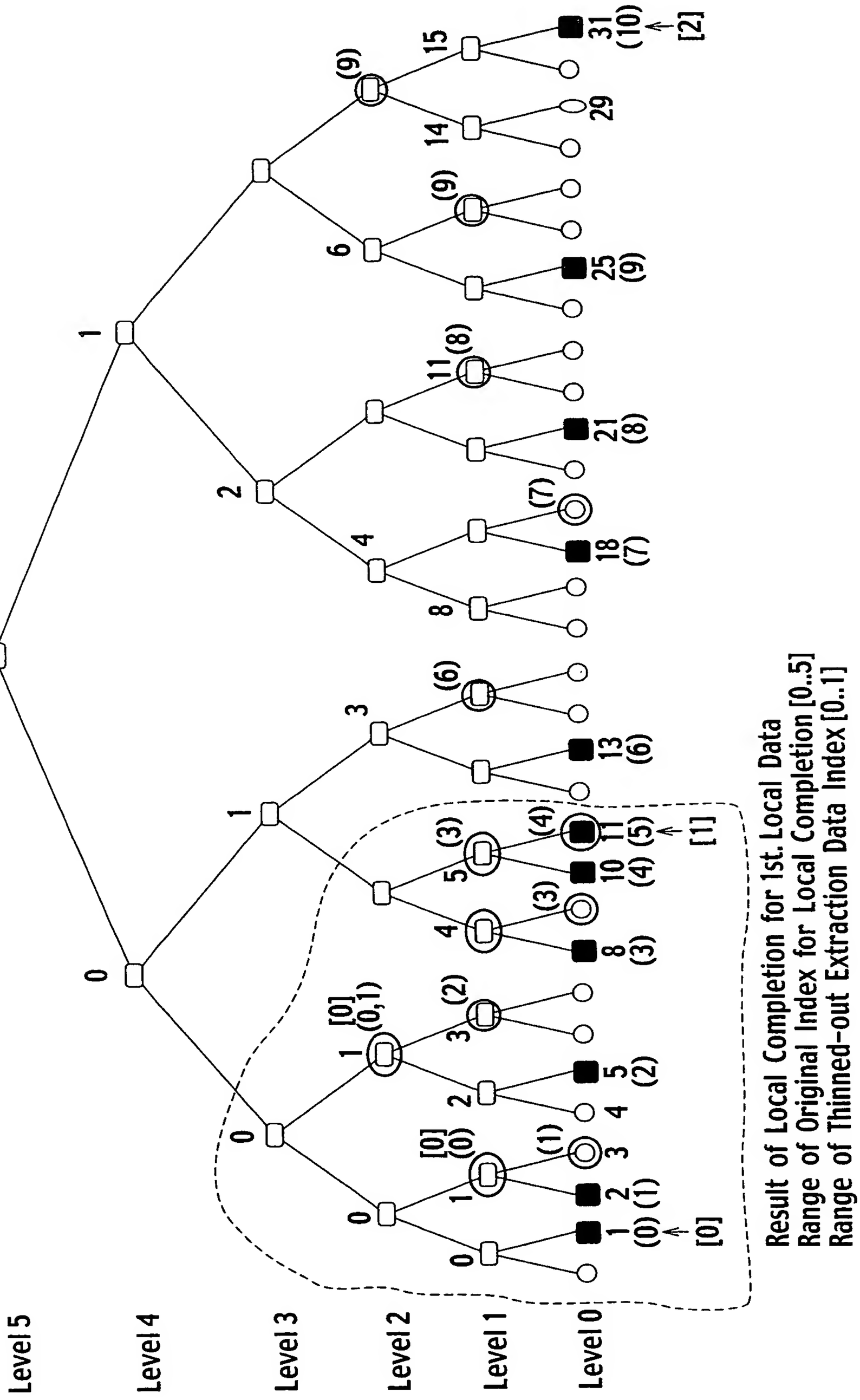
Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 65 of 77

FIG. 71



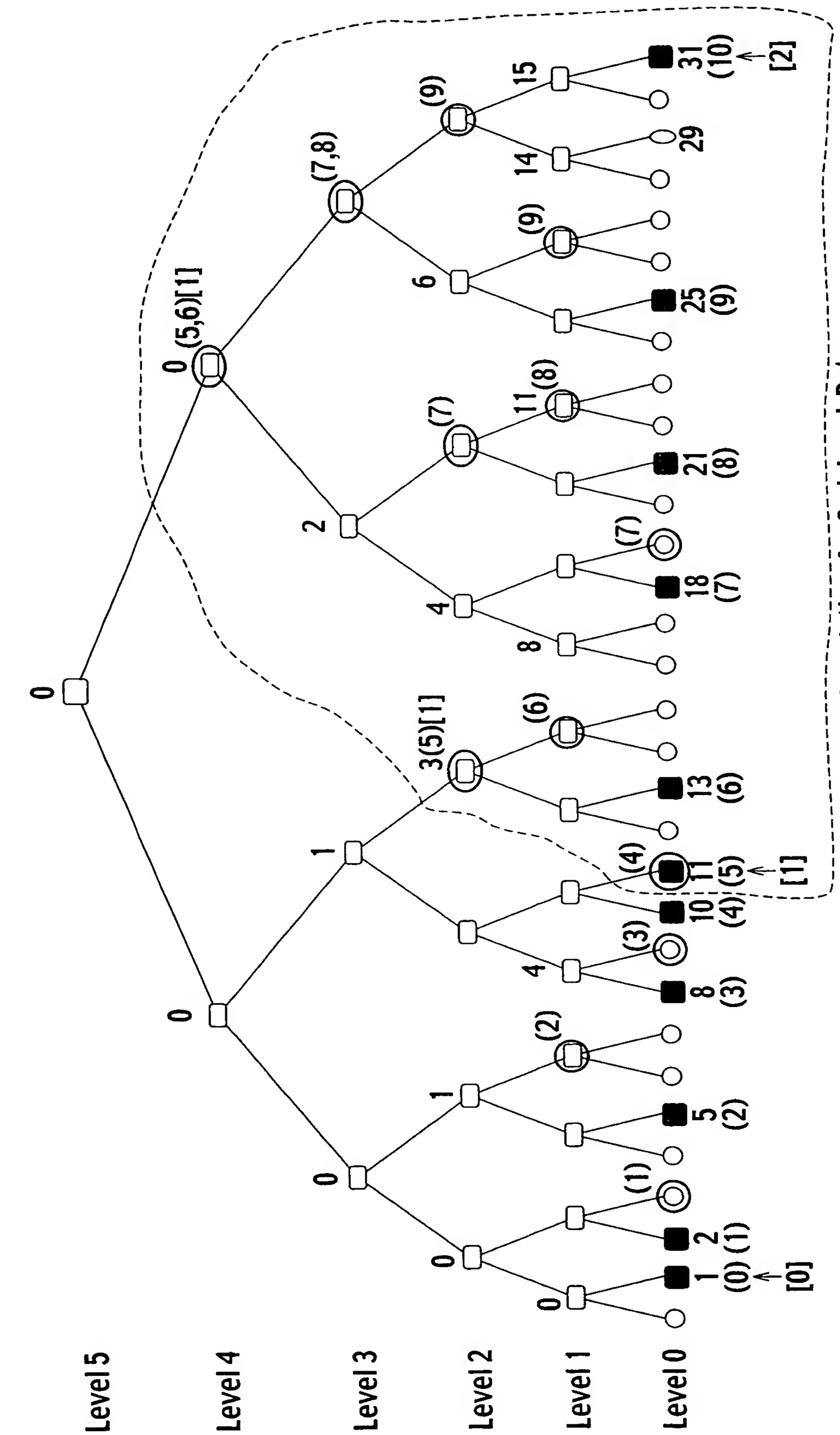
Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 66 of 77

FIG. 72



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 67 of 77

FIG. 73



Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 68 of 77

FIG. 74

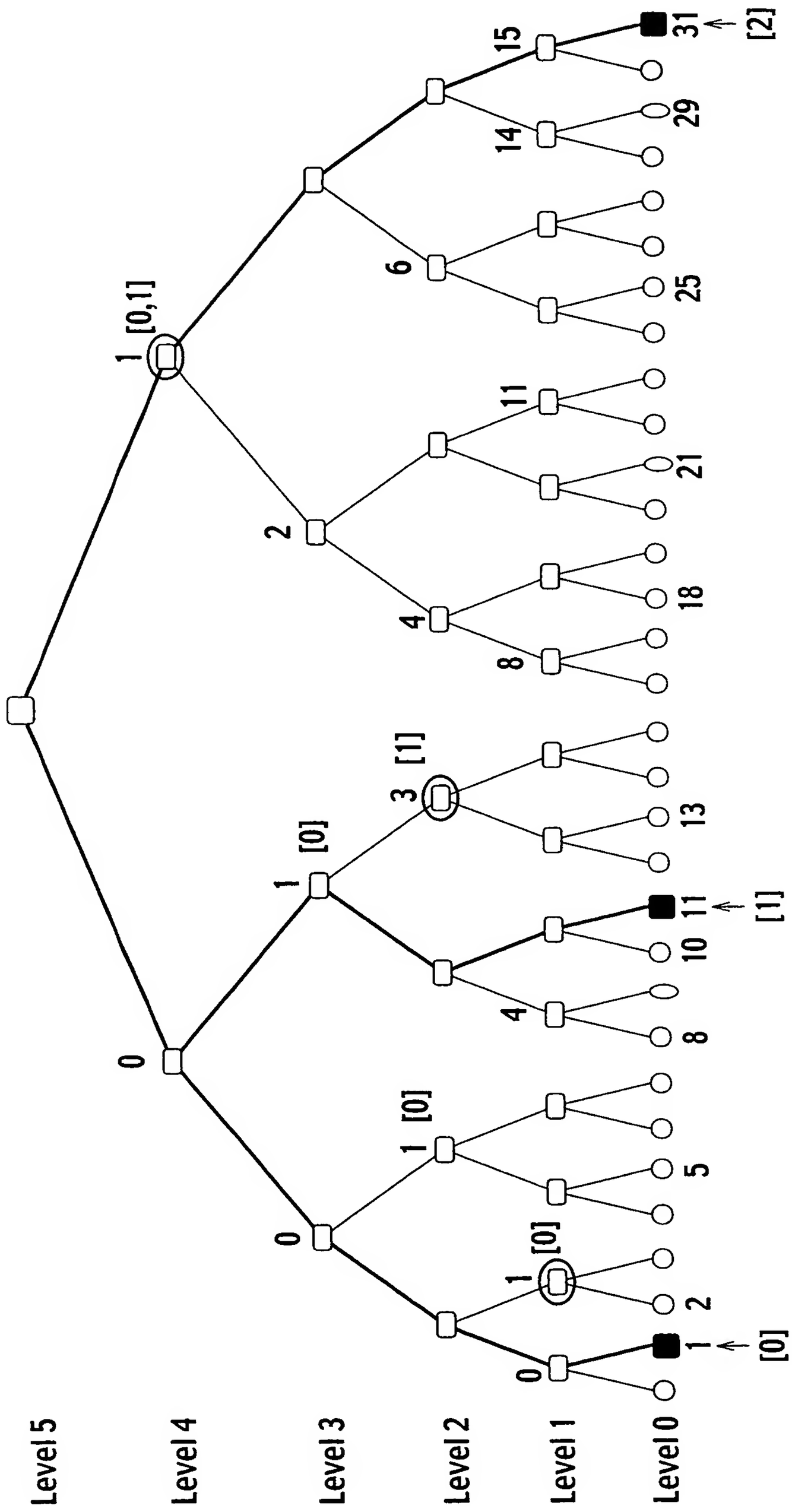
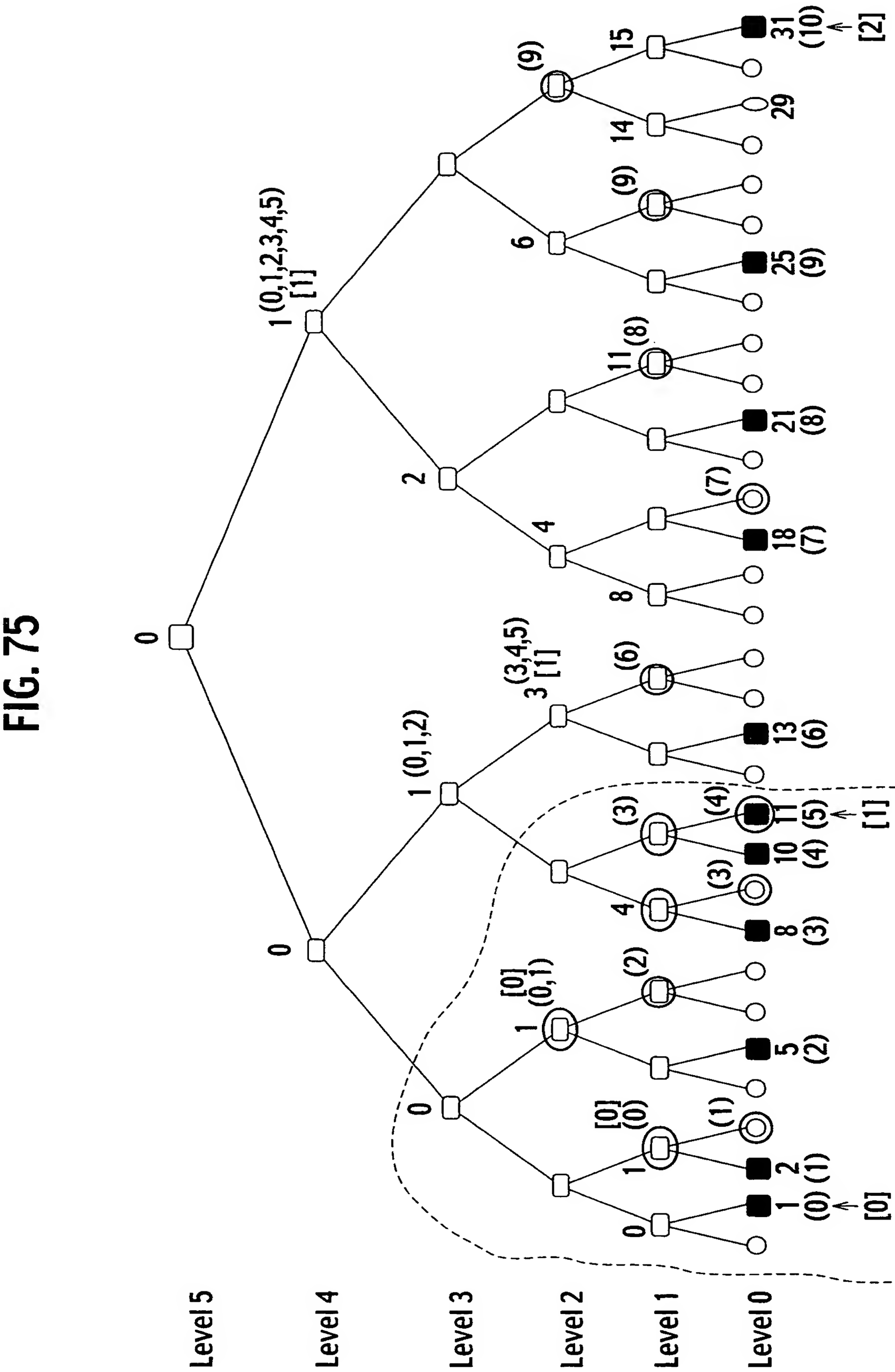


FIG. 75


Level 5
Level 4
Level 3
Level 2
Level 1
Level 0
Result of Global Completion for 1st. Local data
Range of Index for Local Completion [0..5]
[1]
[2]
[0]

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 70 of 77

FIG. 76

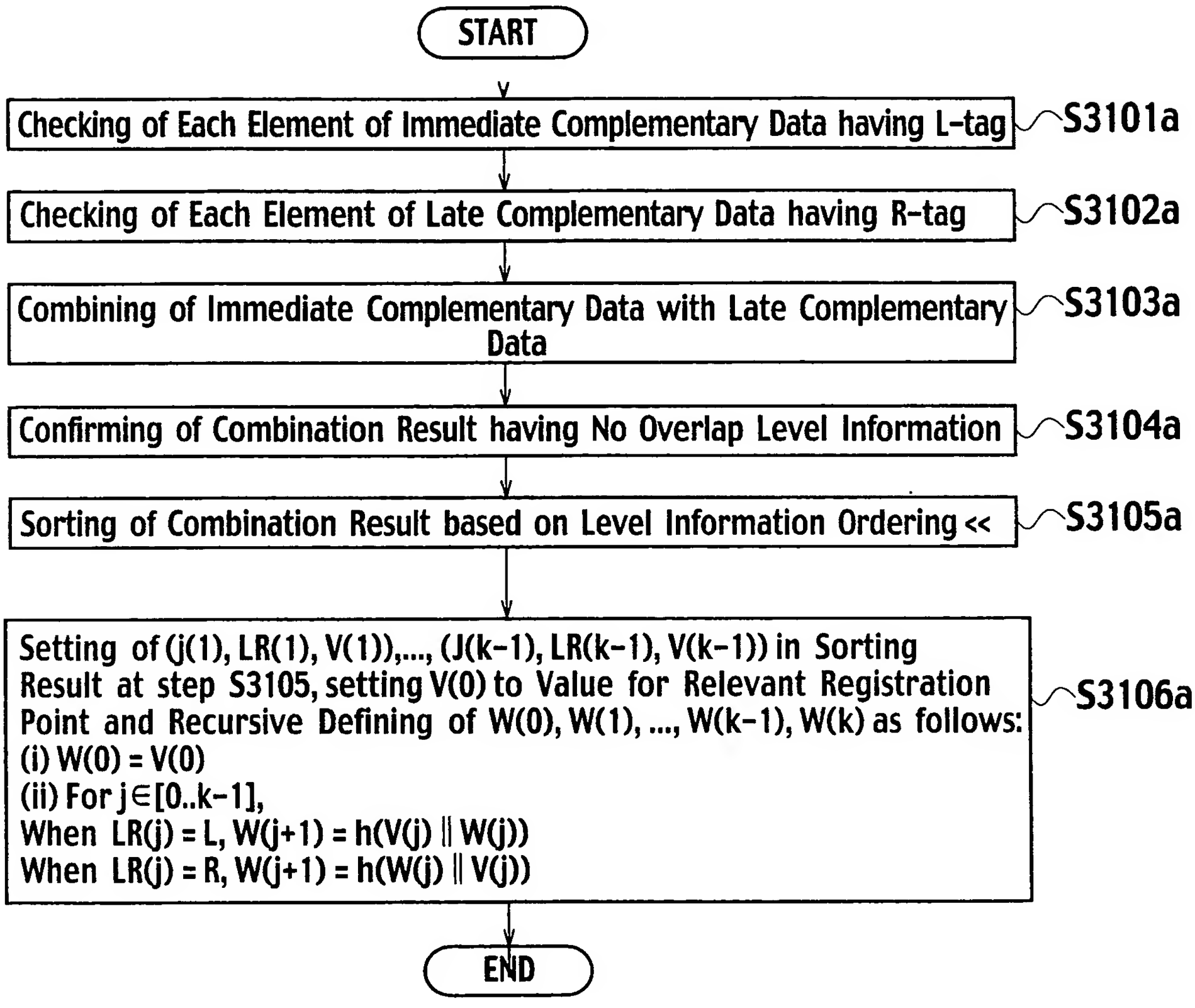


FIG. 77

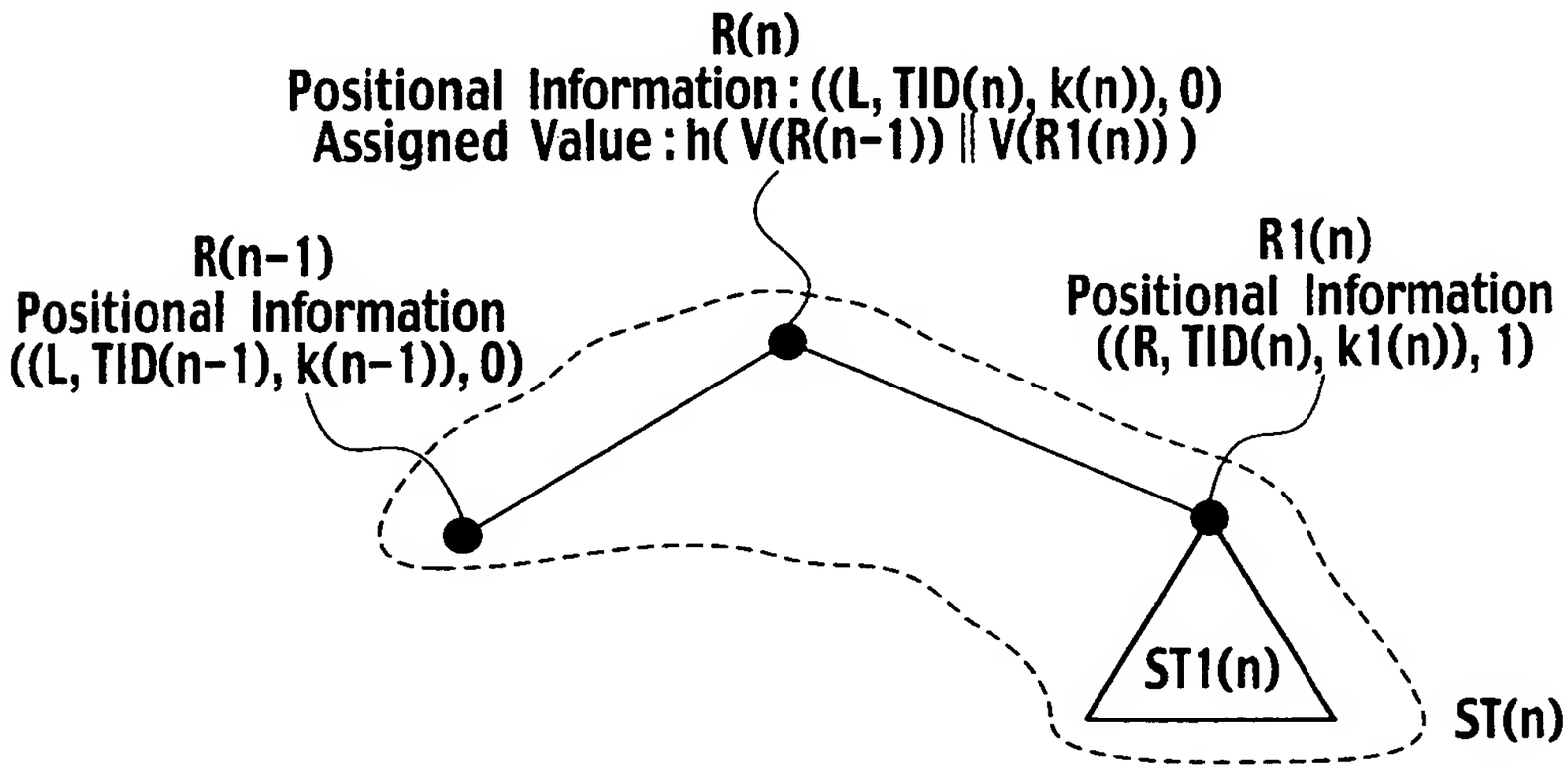


FIG. 78

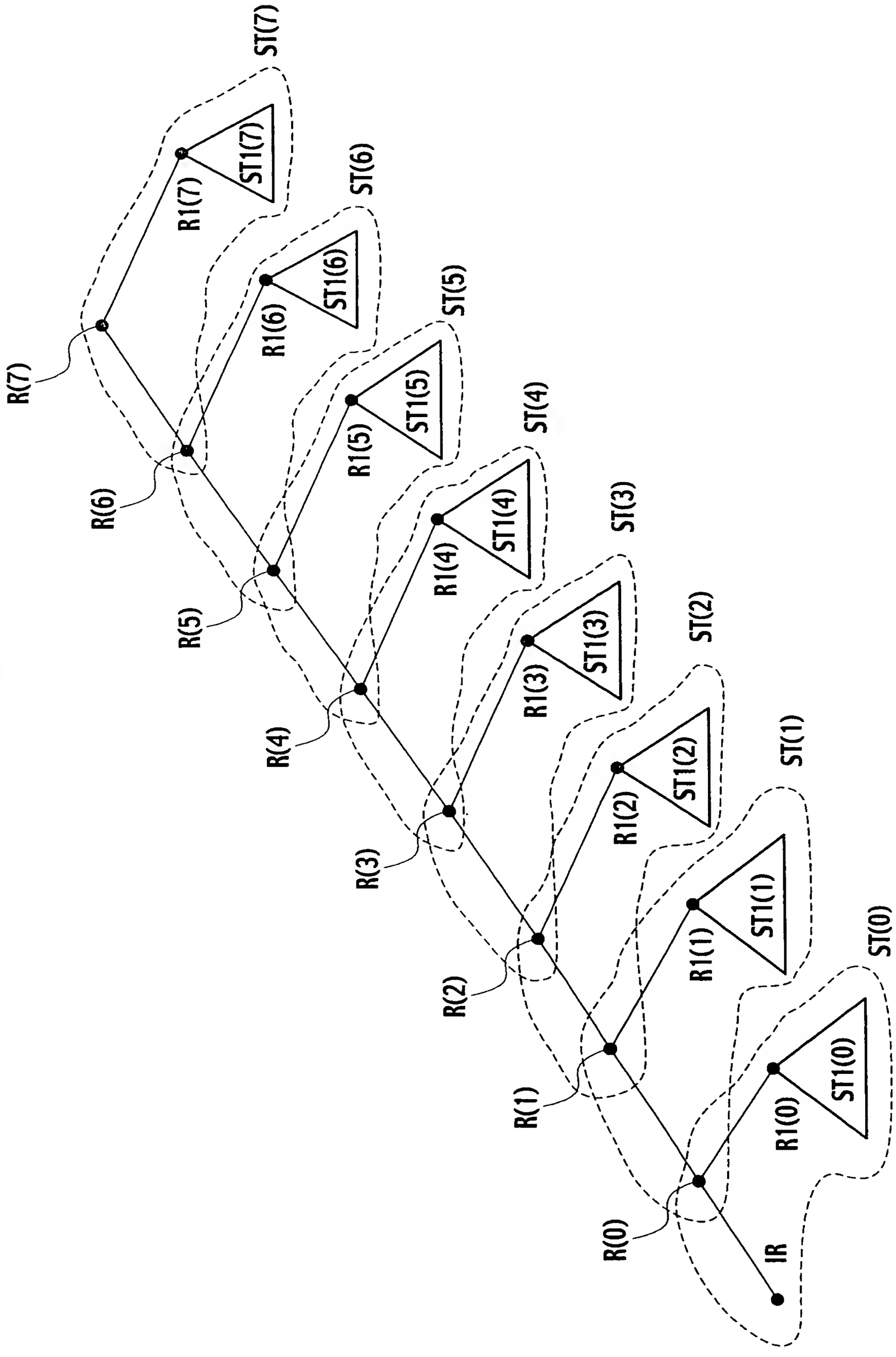

ST(7)
ST1(7)
R1(7)
R(7)
ST(6)
ST1(6)
R1(6)
R(6)
ST(5)
ST1(5)
R1(5)
R(5)
ST(4)
ST1(4)
R1(4)
R(4)
ST(3)
ST1(3)
R1(3)
R(3)
ST(2)
ST1(2)
R1(2)
R(2)
ST(1)
ST1(1)
R1(1)
R(1)
ST(0)
ST1(0)
R1(0)
R(0)
IR

FIG. 79

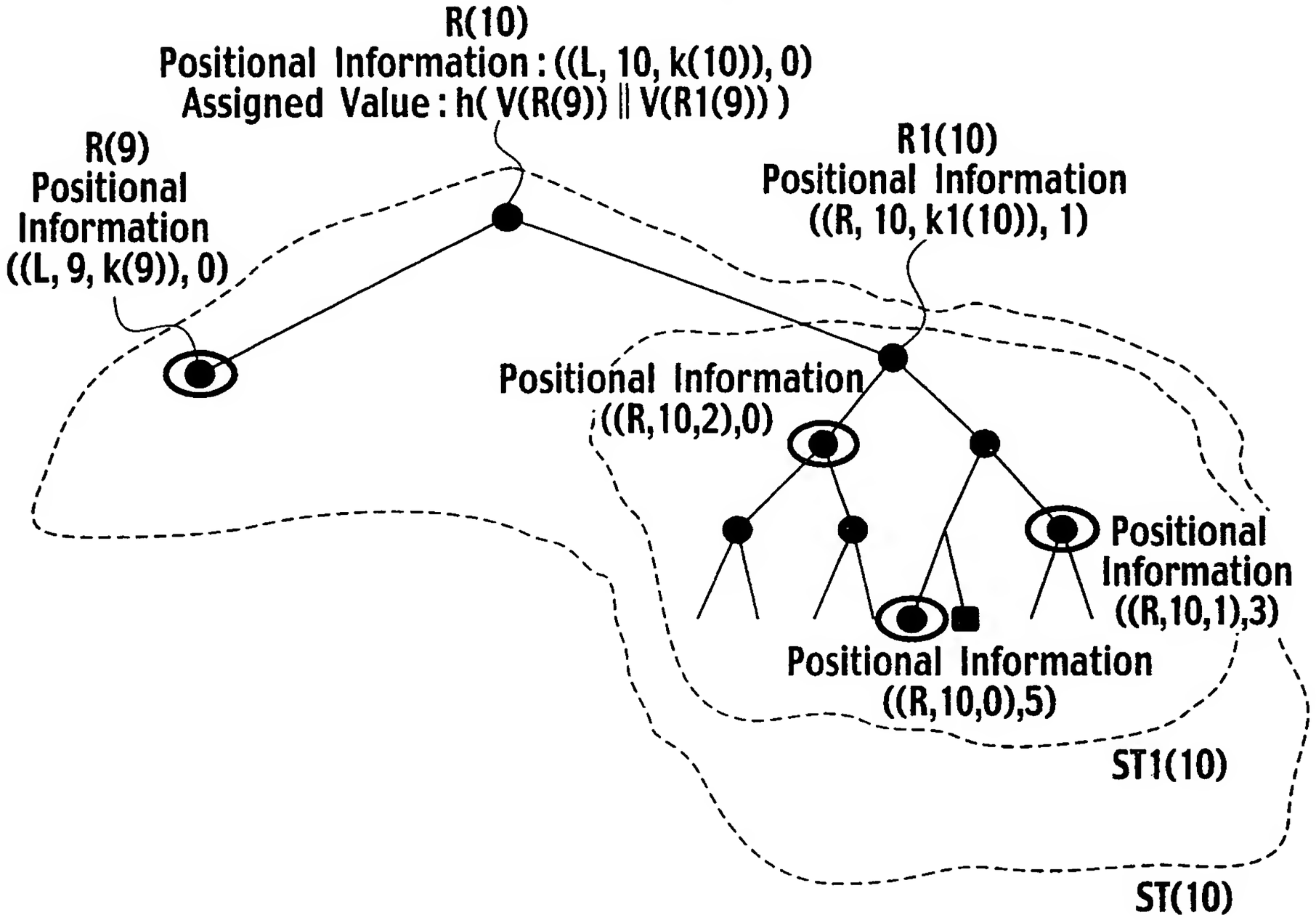

R(10)
Positional Information : ((L, 10, k(10)), 0)
Assigned Value : h(V(R(9)) || V(R1(9)))
R(9)
Positional
Information
((L, 9, k(9)), 0)
R1(10)
Positional Information
((R, 10, k1(10)), 1)
Positional Information
((R,10,2),0)
Positional
Information
((R,10,1),3)
Positional Information
((R,10,0),5)
ST1(10)
ST(10)

FIG. 80

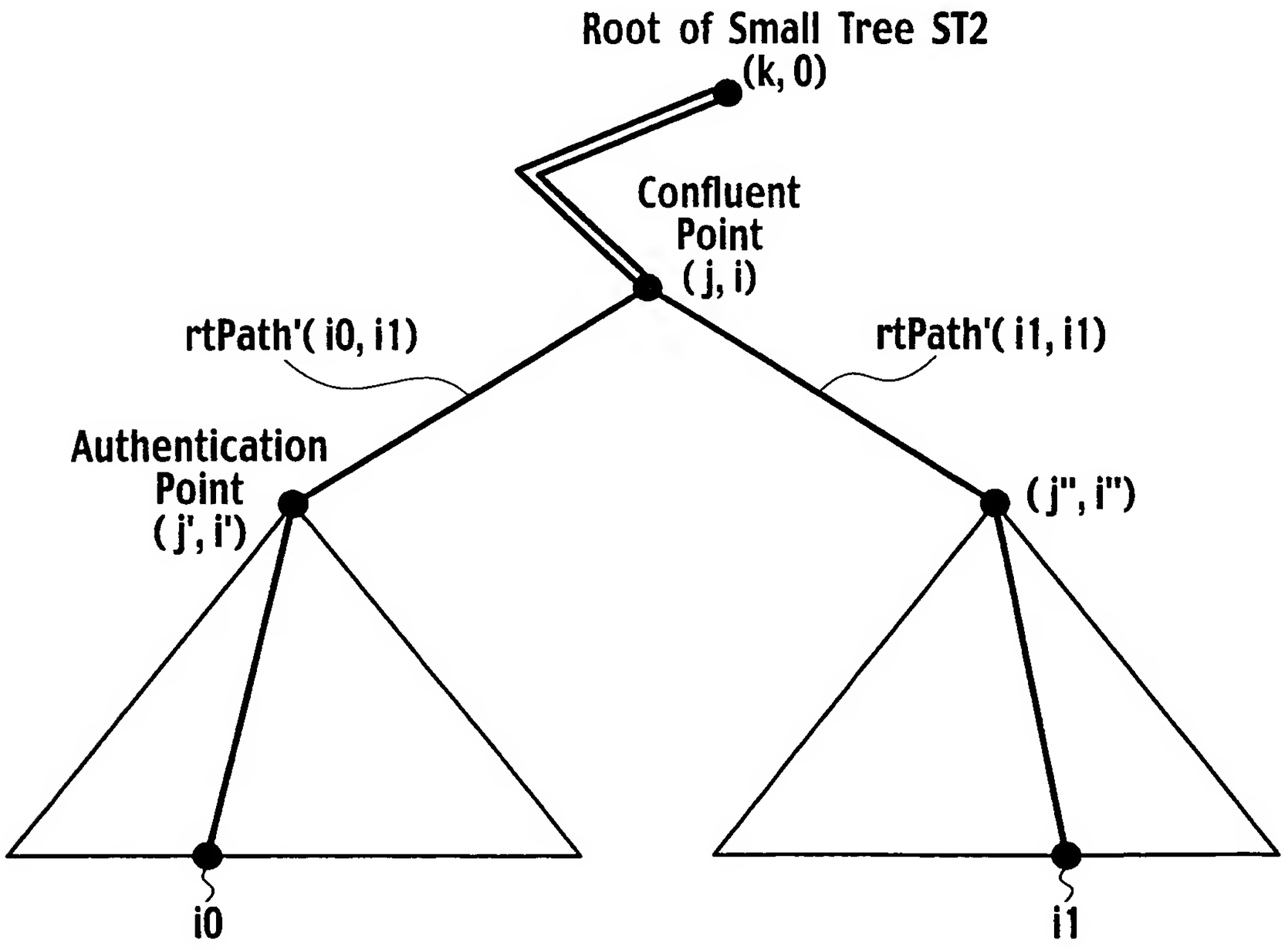

Root of Small Tree ST2
(k, 0)
Confluent
Point
(j, i)
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication
Point
(j', i')
(j'', i'')
i0
i1

FIG. 81

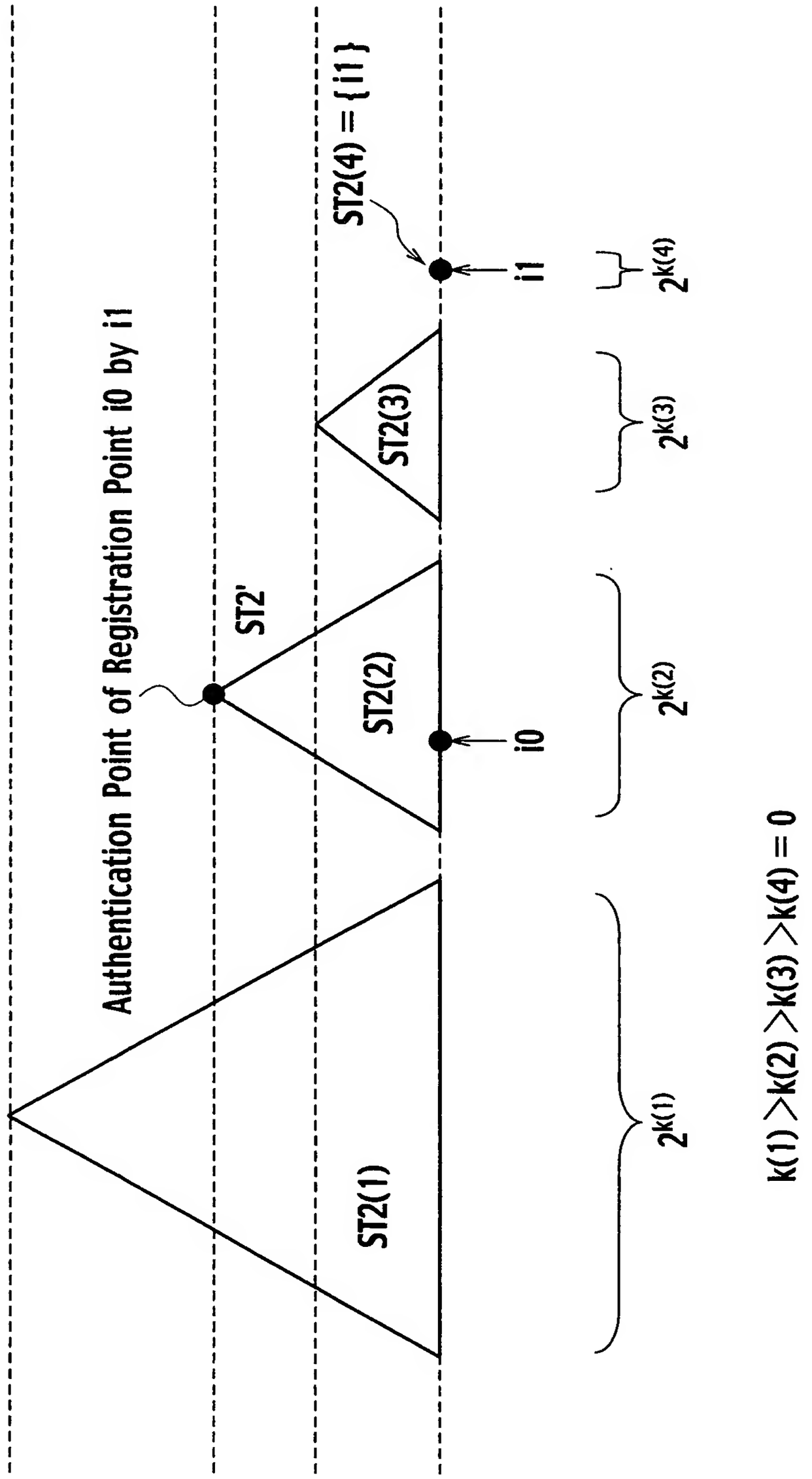

ST2(4) = {i1}
i1
2k(4)
Authentication Point of Registration Point i0 by i1
ST2'
ST2(3)
ST2(2)
i0
2k(3)
2k(2)
ST2(1)
2k(1)
k(1) >k(2) >k(3) >k(4) = 0

FIG. 82

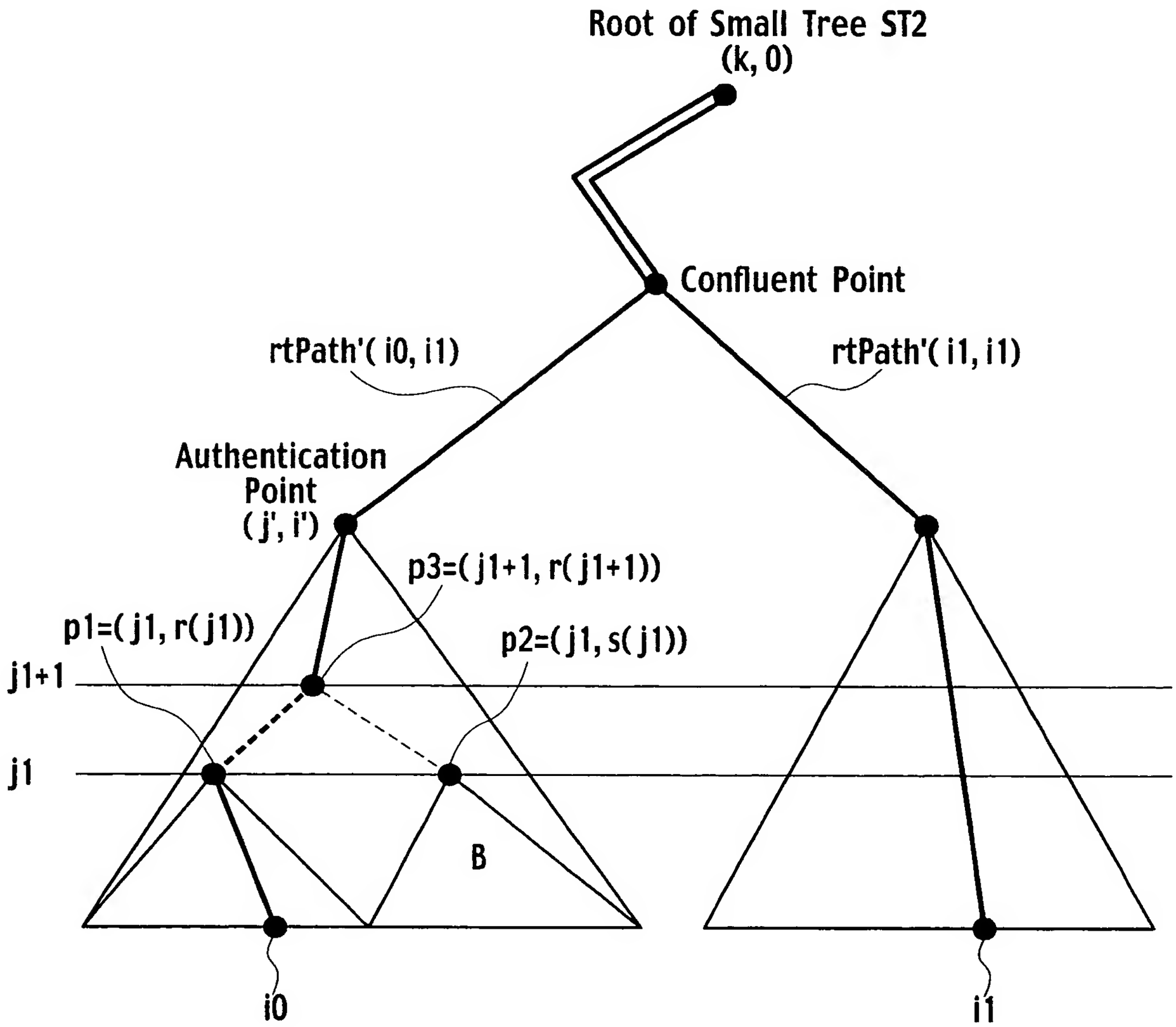

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication
Point
(j', i')
p3=(j1+1, r(j1+1))
p1=(j1, r(j1))
p2=(j1, s(j1))
j1+1
j1
B
i0
i1

FIG. 83

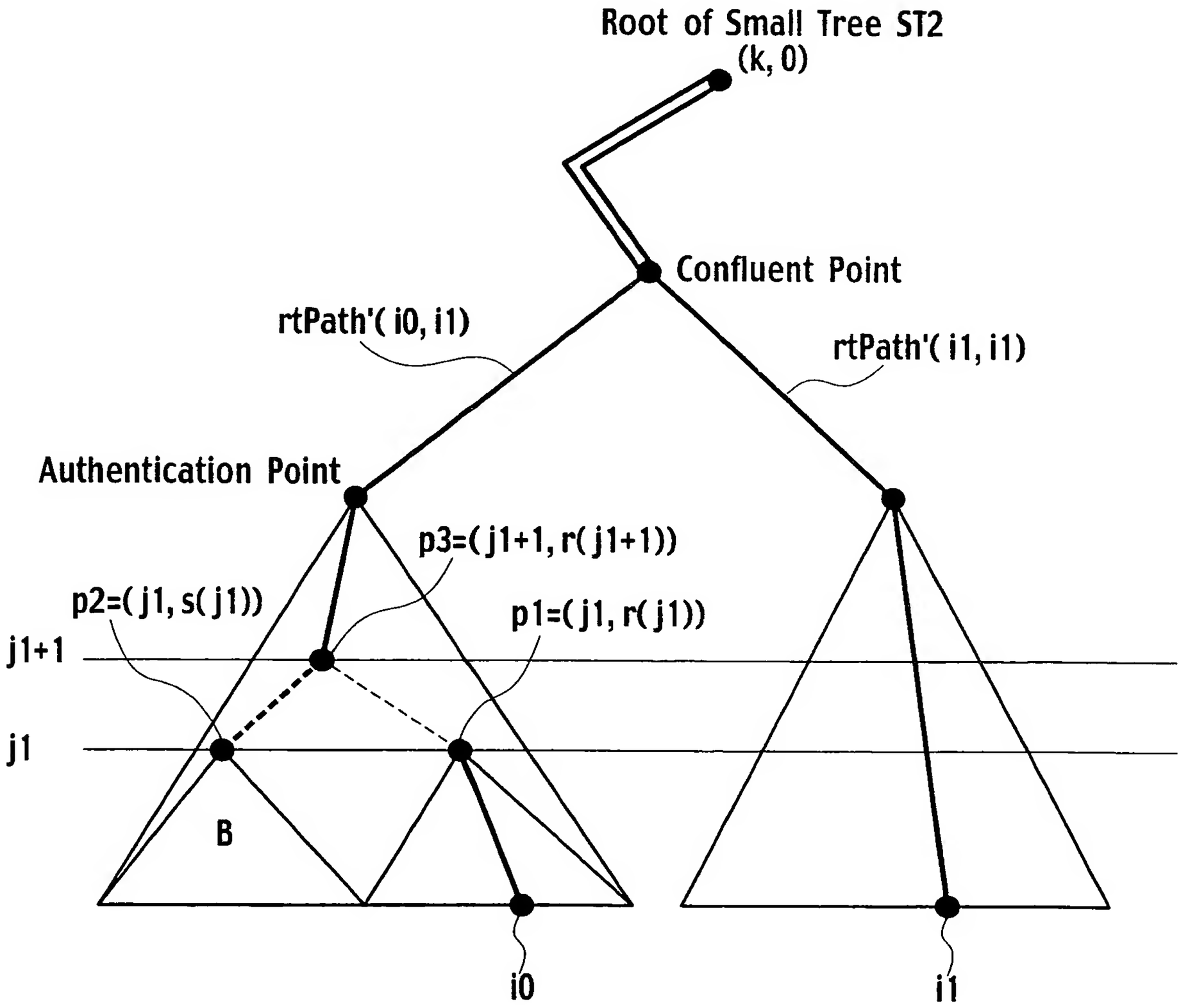
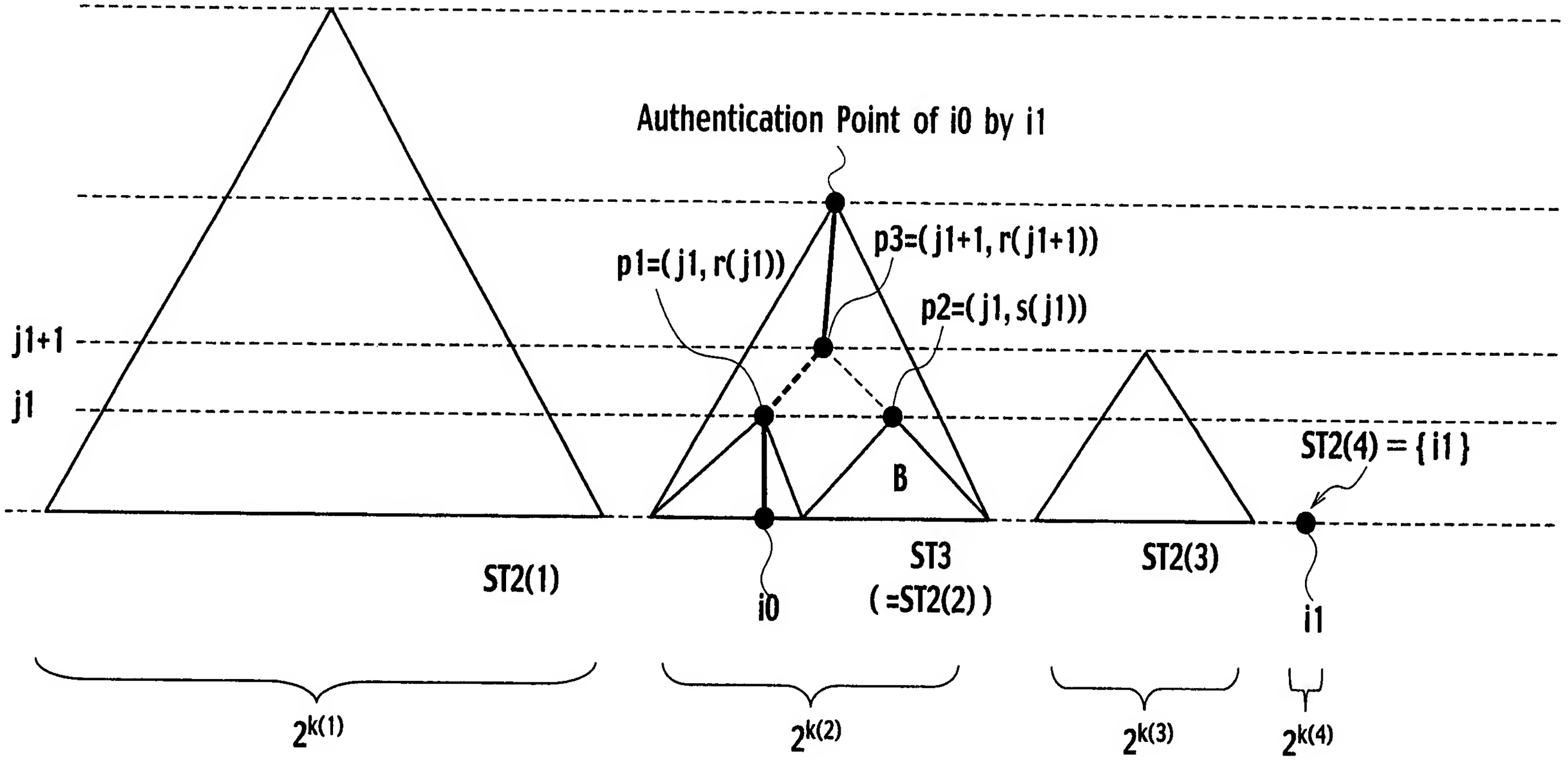

Root of Small Tree ST2
(k, 0)
Confluent Point
rtPath'(i0, i1)
rtPath'(i1, i1)
Authentication Point
p3=(j1+1, r(j1+1))
p2=(j1, s(j1))
p1=(j1, r(j1))
j1+1
j1
B
i0
i1

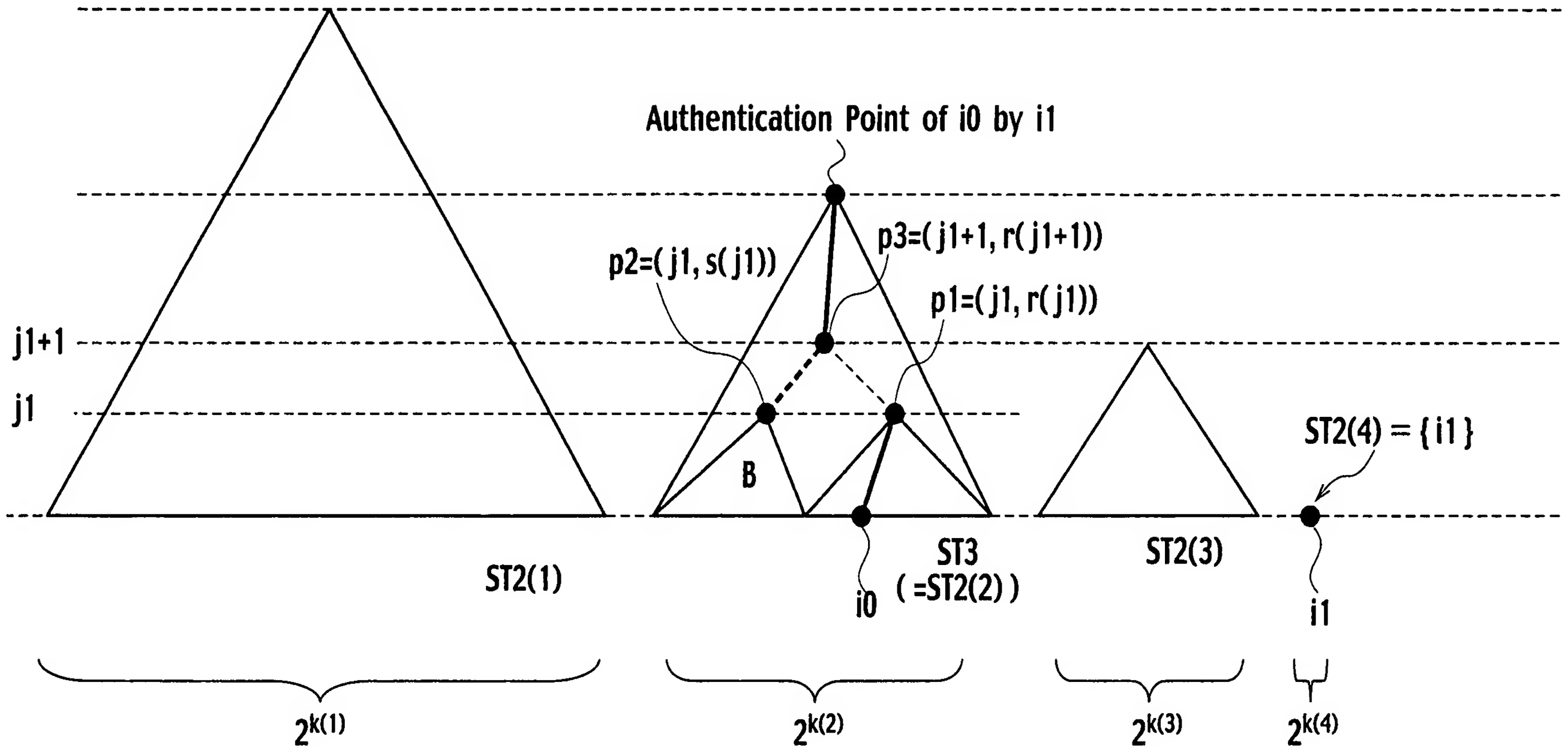
FIG. 84



$k(1) > k(2) > k(3) > k(4) = 0$

Inventors: Fürbi HOBITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 76 of 77

FIG. 85



$k(1) > k(2) > k(3) > k(4) = 0$

Inventors: Eiichi HORITA
Filed: July 21, 2006
Title: Event-Ordering Certification Method
Attorney Docket: 44471/332867
Attorney of Record: Brenda O. Holmes, Reg. No. 40,339
Correspondence Address & POA Customer No. 23370
Phone: 404.815.6500
Sheet 77 of 77